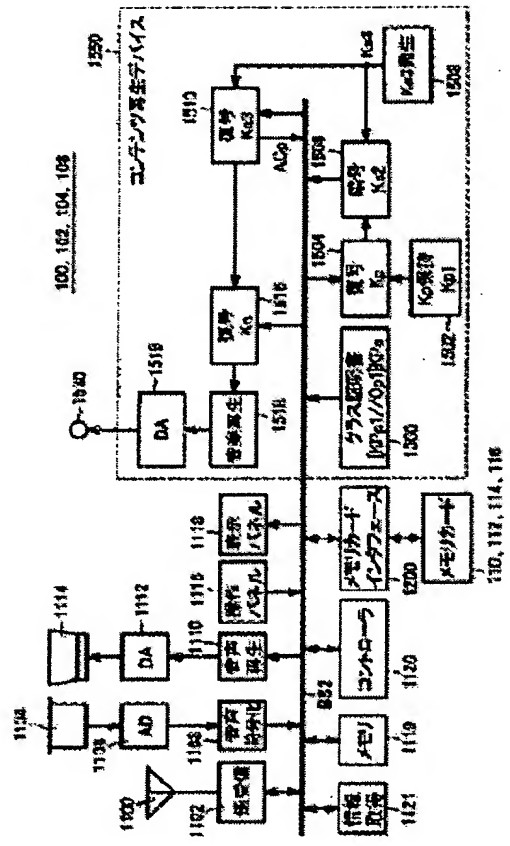
DATA TERMINAL EQUIPMENT AND DATA RE-ACQUIRING METHOD

Publication number: JP2003016288
Publication date: 2003-01-17
Inventor: HIGUCHI GOJI
Applicant: SANYO ELECTRIC CO
Classification:
- international: ***G06Q30/00; G06F12/14; G06F21/24; G06Q10/00; G06Q50/00; G10K15/02; H04L9/08;*** **G06Q30/00; G06F12/14; G06F21/00; G06Q10/00; G06Q50/00; G10K15/02; H04L9/08;** (IPC1-7): G06F17/60; G10K15/02; H04L9/08
- European:
Application number: JP20010199100 20010629
Priority number(s): JP20010199100 20010629

Abstract of **JP2003016288**

PROBLEM TO BE SOLVED: To provide data terminal equipment and a data re-acquiring method with which data terminal equipment acquiring copied contents data can easily re-acquire contents data received before. SOLUTION: A memory 1119 stores a database registering information on a copy source. When the re-acquisition request of copied contents data is inputted through a control panel 1116, a controller 1120 of a portable telephone set 102 accesses a portable telephone set 100 of the copy source on the basis of the information on the copy source stored in the memory 1119 and when the copy of contents data is permitted in the portable telephone set 100, the contents data are re-acquired from the portable telephone set 100.



(19)日本国特許庁（ＪＰ）　(12)**公開特許公報**（Ａ）　(11)特許出願公開番号
特開2003－16288
（P2003－16288A）
(43)公開日　平成15年１月17日(2003.1.17)

(51)Int.Cl.[7]	識別記号	ＦＩ	ﾃｰﾏｺｰﾄﾞ(参考)
Ｇ０６Ｆ　17/60	３０２	Ｇ０６Ｆ　17/60	３０２Ｅ　５Ｊ１０４
	１４２		１４２
	３３６		３３６
	５１２		５１２
	ＺＥＣ		ＺＥＣ

審査請求　有　請求項の数11　ＯＬ　（全 33 頁）　最終頁に続く

(21)出願番号　特願2001－199100(P2001－199100)

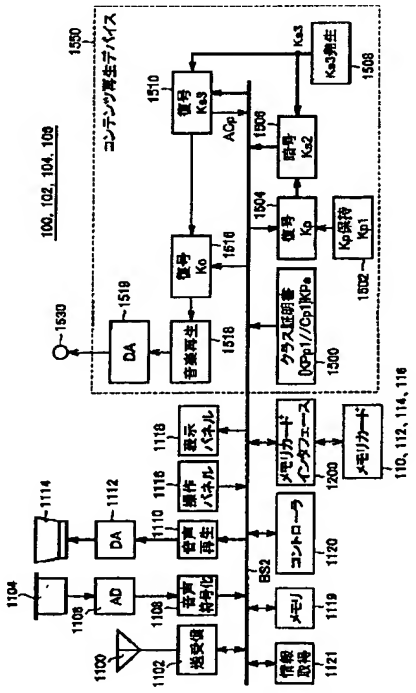
(22)出願日　平成13年６月29日(2001.6.29)

(71)出願人　000001889
三洋電機株式会社
大阪府守口市京阪本通２丁目５番５号
(72)発明者　樋口　剛司
大阪府守口市京阪本通２丁目５番５号　三洋電機株式会社内
(74)代理人　100064746
弁理士　深見　久郎　（外３名）

Ｆターム(参考)　5J104 AA01 AA16 EA01 EA04 NA02 PA14

(54)【発明の名称】　データ端末装置、およびデータ再取得方法

(57)【要約】
【課題】　複製されたコンテンツデータを受信したデータ端末装置が以前に受信したコンテンツデータを容易に再取得できるデータ端末装置およびデータ再取得方法を提供する。
【解決手段】　メモリ１１１９は複製元に関する情報が登録されたデータベースを格納する。携帯電話機１０２のコントローラ１１２０は、複製されたコンテンツデータの再取得要求が操作パネル１１１６を介して入力されると、メモリ１１１９に格納された複製元に関する情報に基づいて複製元である携帯電話機１００へアクセスし、携帯電話機１００においてコンテンツデータの複製が許可されたとき、コンテンツデータを携帯電話機１００から再取得する。



1

【特許請求の範囲】

【請求項１】　複製されたコンテンツデータと前記コンテンツデータの付加情報と前記コンテンツデータの複製元の固有情報とを含むデータを受信し、前記複製元に関する情報を管理するデータ端末装置であって、
前記コンテンツデータを記録するデータ記録装置との間でデータのやり取りを行なうインタフェースと、
外部とのデータのやり取りを行なう送受信手段と、
前記複製元に関する情報を管理する情報管理手段と、
前記データから前記コンテンツデータと前記固有情報と前記付加情報とを取得する取得手段と、
制御手段とを備え、
前記制御手段は、前記送受信手段を介して前記データを受信すると、その受信したデータを前記取得手段に与え、前記取得手段により取得されたコンテンツデータを前記インタフェースを介して前記データ記録装置に記録し、前記取得手段により取得された固有情報と付加情報とを前記複製元に関する情報として前記情報管理手段に格納する、データ端末装置。

【請求項２】　複製されたコンテンツデータおよび前記コンテンツデータの付加情報を含むデータと、前記コンテンツデータの複製元にアクセスするアクセス情報とを受信し、前記複製元に関する情報を管理するデータ端末装置であって、
前記コンテンツデータを記録するデータ記録装置との間でデータのやり取りを行なうインタフェースと、
外部とのデータのやり取りを行なう送受信手段と、
前記複製元に関する情報を管理する情報管理手段と、
前記複製元の固有情報を生成する情報生成手段と、
前記データから前記コンテンツデータと前記付加情報とを取得する取得手段と、
制御手段とを備え、
前記制御手段は、前記送受信手段を介して前記データを受信すると、その受信したデータを前記取得手段に与え、前記送受信手段を介して受信したアクセス情報を前記情報生成手段に与え、前記取得手段により取得されたコンテンツデータを前記インタフェースを介して前記データ記録装置に記録し、前記情報生成手段によって生成された固有情報と前記取得手段により取得された付加情報とを前記複製元に関する情報として前記情報管理手段に格納し、
前記情報生成手段は、前記与えられたアクセス情報を用いて前記固有情報を生成し、その生成した固有情報を前記制御手段に与える、データ端末装置。

【請求項３】　指示を入力するためのキー操作手段と、各種の情報を視覚情報としてユーザに表示する表示手段とをさらに備え、
前記制御手段は、前記キー操作手段を介して入力された前記複製元に関する情報の表示要求に応じて、前記情報管理手段から前記複製元に関する情報を読出して前記表

2

示手段に与え、前記表示手段によって表示された複製元に関する情報に含まれる付加情報に対応するコンテンツデータの再取得要求が前記キー操作手段を介して入力されると、前記固有情報に含まれるアクセス情報を用いて前記複製元のデータ端末装置から前記コンテンツデータを再取得し、
前記表示手段は、前記複製元に対応する情報を表示する、請求項１または請求項２に記載のデータ端末装置。

【請求項４】　指示を入力するためのキー操作手段と、各種の情報を視覚情報としてユーザに表示する表示手段とをさらに備え、
前記情報管理手段は、前記複製元のデータ端末装置から受信したコンテンツデータの個数に応じた複数の複製元に関する情報を管理し、
前記制御手段は、前記キー操作手段を介して入力された前記複製元に関する情報の表示要求に応じて、前記情報管理手段から前記複数の複製元に関する情報を読出して前記表示手段に与え、前記表示手段によって表示された複数の複製元に関する情報のうちユーザによって選択された複製元に関する情報に含まれる付加情報に対応するコンテンツデータの再取得要求が前記キー操作手段を介して入力されると、前記固有情報に含まれるアクセス情報を用いて前記選択されたコンテンツデータの複製元のデータ端末装置から前記コンテンツデータを再取得し、
前記表示手段は、前記複数の複製元に対応する情報を表示する、請求項１または請求項２に記載のデータ端末装置。

【請求項５】　前記制御手段は、前記複製元のデータ端末装置がコンテンツデータの複製に応じたとき、前記送受信手段を介して前記複製元のデータ端末装置から前記コンテンツデータを再取得する、請求項３または請求項４に記載のデータ端末装置。

【請求項６】　前記コンテンツデータは、ライセンス鍵によって暗号化された暗号化コンテンツデータであり、
前記制御手段は、前記キー操作手段を介して入力された前記ライセンス鍵を含むライセンスの配信要求に応じて、前記ライセンスを保持するサーバへアクセスし、前記サーバから前記ライセンスを受信する、請求項１から請求項５のいずれか１項に記載のデータ端末装置。

【請求項７】　複製されたコンテンツデータと前記コンテンツデータの付加情報と前記コンテンツデータの複製元の固有情報とを含むデータを受信し、前記付加情報および前記固有情報を前記コンテンツデータの複製元に関する情報として管理するデータ端末装置において前記コンテンツデータを前記複製元のデータ端末装置から再取得するデータ再取得方法であって、
前記受信した複製元に関する情報を表示手段に表示する第１のステップと、
前記表示された複製元に関する情報に含まれる付加情報に対応するコンテンツデータの再取得要求を受付ける第

２のステップと、
前記表示された複製元に関する情報に含まれる固有情報に基づいて再取得要求がなされたコンテンツデータの複製元にアクセスし、前記複製元のデータ端末装置から複製されたコンテンツデータを再取得する第３のステップとを含むデータ再取得方法。
【請求項８】　複製されたコンテンツデータおよび前記コンテンツデータの付加情報を含むデータと、前記コンテンツデータの複製元にアクセスするアクセス情報とを受信し、前記付加情報と前記受信したアクセス情報を用いて生成された前記複製元の固有情報とを前記複製元に関する情報として管理するデータ端末装置において前記コンテンツデータを前記複製元のデータ端末装置から再取得するデータ再取得方法であって、
前記受信した複製元に関する情報を表示手段に表示する第１のステップと、
前記表示された複製元に関する情報に含まれる付加情報に対応するコンテンツデータの再取得要求を受付ける第２のステップと、
前記表示された複製元に関する情報に含まれる固有情報に基づいて再取得要求がなされたコンテンツデータの複製元にアクセスし、前記複製元のデータ端末装置から複製されたコンテンツデータを再取得する第３のステップとを含むデータ再取得方法。
【請求項９】　前記第１のステップにおいて、前記複製元のデータ端末装置から受信したコンテンツデータの個数に応じた複数の複製元に関する情報を表示し、
前記第２のステップにおいて、前記表示された複数の複製元に関する情報のうちユーザによって選択された複製元に関する情報に含まれる付加情報に対応するコンテンツデータの再取得要求が受付けられる、請求項７または請求項８に記載のデータ再取得方法。
【請求項１０】　前記第３のステップにおいて、前記複製元のデータ端末装置が前記コンテンツデータの複製を許可したとき、前記複製元のデータ端末装置から前記コンテンツデータを再取得する、請求項７から請求項９のいずれか１項に記載のデータ再取得方法。
【請求項１１】　前記コンテンツデータは、ライセンス鍵によって暗号化された暗号化コンテンツデータであり、
前記ライセンス鍵を含むライセンスの配信要求を受付ける第４のステップと、
前記ライセンスを保持するサーバへアクセスし、前記サーバから前記ライセンスを受信する第５のステップとをさらに含む、請求項７から請求項１０のいずれか１項に記載のデータ再取得方法。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】この発明は、コピーされた情報に対する著作権保護を可能とするデータ配信システムにおいて用いられるデータ端末装置、およびデータ再取得方法に関するものである。
【０００２】
【従来の技術】近年、インターネット等の情報通信網等の進歩により、携帯電話機等を用いた個人向け端末により、各ユーザが容易にネットワーク情報にアクセスすることが可能となっている。
【０００３】このような情報通信網においては、デジタル信号により情報が伝送される。したがって、たとえば上述のような情報通信網において伝送された音楽や映像データを各個人ユーザがコピーした場合でも、そのようなコピーによる音質や画質の劣化をほとんど生じさせることなく、データのコピーを行なうことが可能である。
【０００４】したがって、このような情報通信網上において音楽データや画像データ等の著作者の権利が存在する創作物が伝達される場合、適切な著作権保護のための方策が取られていないと、著しく著作権者の権利が侵害されてしまうおそれがある。
【０００５】一方で、著作権保護の目的を最優先して、急拡大するデジタル情報通信網を介して著作物データの配信を行なうことができないとすると、基本的には、著作物データの複製に際し一定の著作権料を徴収することが可能な著作権者にとっても、かえって不利益となる。
【０００６】ここで、上述のようなデジタル情報通信網を介した配信ではなく、デジタルデータを記録した記録媒体を例にとって考えて見ると、通常販売されている音楽データを記録したＣＤ（コンパクトディスク）については、ＣＤから光磁気ディスク（ＭＤ等）への音楽データのコピーは、当該コピーした音楽を個人的な使用に止める限り原則的には自由に行なうことができる。ただし、デジタル録音等を行なう個人ユーザは、デジタル録音機器自体やＭＤ等の媒体の代金のうちの一定額を間接的に著作権者に対して保証金として支払うことになっている。
【０００７】しかも、ＣＤからＭＤへデジタル信号である音楽データをコピーした場合、これらの情報がコピー劣化の殆どないデジタルデータであることに鑑み、記録可能なＭＤからさらに他のＭＤに音楽情報をデジタルデータとしてコピーすることは、著作権保護のために機器の構成上できないようになっている。
【０００８】このような事情からも、音楽データや画像データをデジタル情報通信網を通じて公衆に配信することは、それ自体が著作権者の公衆送信権による制限を受ける行為であるから、著作権保護のための十分な方策が講じられる必要がある。
【０００９】この場合、情報通信網を通じて公衆に送信される著作物である音楽データや画像データ等のコンテンツデータについて、一度受信されたコンテンツデータが、さらに勝手に複製されることを防止することが必要となる。

【００１０】そこで、コンテンツデータを暗号化した暗号化コンテンツデータを保持する配信サーバが、携帯電話機等の端末装置に装着されたメモリカードに対して端末装置を介して暗号化コンテンツデータを配信するデータ配信システムが提案されている。このデータ配信システムにおいては、予め認証局で認証されたメモリカードの公開暗号鍵とその証明書を暗号化コンテンツデータの配信要求の際に配信サーバへ送信し、配信サーバが認証された証明書を受信したことを確認した上でメモリカードに対して暗号化コンテンツデータと、暗号化コンテンツデータを復号するためのライセンス鍵を送信する。そして、暗号化コンテンツデータやライセンス鍵を配信する際、配信サーバおよびメモリカードは、配信毎に異なるセッションキーを発生させ、その発生させたセッションキーによって公開暗号鍵の暗号化を行ない、配信サーバ、メモリカード相互間で鍵の交換を行なう。

【００１１】最終的に、配信サーバは、メモリカード個々の公開暗号鍵によって暗号化され、さらにセッションキーによって暗号化したライセンスと、暗号化コンテンツデータをメモリカードに送信する。そして、メモリカードは、受信したライセンス鍵と暗号化コンテンツデータをメモリカードに記録する。

【００１２】そして、メモリカードに記録した暗号化コンテンツデータを再生するときは、メモリカードを携帯電話機に装着する。携帯電話機は、通常の電話機能の他にメモリカードからの暗号化コンテンツデータを復号し、かつ、再生して外部へ出力するための専用回路も有する。

【００１３】このように、携帯電話機のユーザは、携帯電話機を用いて暗号化コンテンツデータを配信サーバから受信し、その暗号化コンテンツデータを再生することができる。

【００１４】また、携帯電話機のユーザは、受信した暗号化コンテンツデータを聴いてみて良かったので、その受信した暗号化コンテンツデータを友人にプレゼントしたい場合もある。その場合、携帯電話機のユーザは、受信した暗号化コンテンツデータを友人の携帯電話機へ送信することによって暗号化コンテンツデータを複製する。

【００１５】友人の携帯電話機は、暗号化コンテンツデータを受信し、その受信した暗号化コンテンツデータを装着されたメモリカードに記録する。そして、友人は、プレゼントされた暗号化コンテンツデータを復号および再生するためのライセンスを配信サーバから取得する指示を自己の携帯電話機に与え、携帯電話機は、そのライセンスを配信サーバから受信してメモリカードに記録する。これによって、友人は、プレゼントされた暗号化コンテンツデータを復号および再生して聴くことができる。また、暗号化コンテンツデータを、友人の携帯電話機からコピーすることもできる。この場合はユーザが自分の携帯電話機を操作して、友人の携帯電話機に回線を接続して、友人の携帯電話機のメモリカードに記録された暗号化コンテンツデータを自分の携帯電話機のメモリカードに複製する。この場合、暗号化コンテンツデータの複製は自由に行なわれるが、暗号化コンテンツデータをプレゼントされた／複製したユーザは、そのままでは暗号化コンテンツデータを復号および再生できず、配信サーバから暗号化コンテンツデータを復号および再生するためのライセンスを購入する必要がある。したがって、暗号化コンテンツデータの複製が自由に行なわれても、暗号化コンテンツデータの著作者の著作権は保護されている。

【００１６】

【発明が解決しようとする課題】しかし、暗号化コンテンツデータをプレゼントされたユーザが、そのプレゼントされた／複製した暗号化コンテンツデータを復号および再生した後に、もう必要がないと思ってプレゼントされた暗号化コンテンツデータをメモリカードから削除することがある。そして、削除した後に、再度、以前にプレゼントされた／複製した暗号化コンテンツデータが必要になることがある。このような場合、暗号化コンテンツデータを配信サーバから受信するのでは、配信サーバとの通信時間が長くなり、手続きも煩雑であるという問題がある。

【００１７】そこで、本発明は、かかる問題を解決するためになされたものであり、その目的は、複製されたコンテンツデータを受信したデータ端末装置が以前に受信したコンテンツデータを容易に再取得できるデータ端末装置およびデータ再取得方法を提供することである。

【００１８】

【課題を解決するための手段】この発明によれば、データ端末装置は、複製されたコンテンツデータとコンテンツデータの付加情報とコンテンツデータの複製元の固有情報とを含むデータを受信し、複製元に関する情報を管理するデータ端末装置であって、コンテンツデータを記録するデータ記録装置との間でデータのやり取りを行なうインタフェースと、外部とのデータのやり取りを行なう送受信手段と、複製元に関する情報を管理する情報管理手段と、データからコンテンツデータと固有情報と付加情報とを取得する取得手段と、制御手段とを備え、制御手段は、送受信手段を介してデータを受信すると、その受信したデータを取得手段に与え、取得手段により取得されたコンテンツデータをインタフェースを介してデータ記録装置に記録し、取得手段により取得された固有情報と付加情報とを複製元に関する情報として情報管理手段に格納する。

【００１９】したがって、この発明によれば、複製先のデータ端末装置は、コンテンツデータの複製により複製元の固有情報を取得できる。

【００２０】また、この発明によれば、データ端末装置

は、複製されたコンテンツデータおよびコンテンツデータの付加情報を含むデータと、コンテンツデータの複製元にアクセスするアクセス情報とを受信し、複製元に関する情報を管理するデータ端末装置であって、コンテンツデータを記録するデータ記録装置との間でデータのやり取りを行なうインタフェースと、外部とのデータのやり取りを行なう送受信手段と、複製元に関する情報を管理する情報管理手段と、複製元の固有情報を生成する情報生成手段と、データから前記コンテンツデータと付加情報とを取得する取得手段と、制御手段とを備え、制御手段は、送受信手段を介してデータを受信すると、その受信したデータを取得手段に与え、送受信手段を介して受信したアクセス情報を情報生成手段に与え、取得手段により取得されたコンテンツデータをインタフェースを介してデータ記録装置に記録し、情報生成手段によって生成された固有情報と取得手段により取得された付加情報とを複製元に関する情報として情報管理手段に格納し、情報生成手段は、与えられたアクセス情報を用いて固有情報を生成し、その生成した固有情報を制御手段に与える。

【００２１】したがって、この発明によれば、複製先のデータ端末装置は、複製元の固有情報を自ら生成できる。

【００２２】好ましくは、データ端末装置は、指示を入力するためのキー操作手段と、各種の情報を視覚情報としてユーザに表示する表示手段とをさらに備え、制御手段は、キー操作手段を介して入力された複製元に関する情報の表示要求に応じて、情報管理手段から複製元に関する情報を読出して表示手段に与え、表示手段によって表示された複製元に関する情報に含まれる付加情報に対応するコンテンツデータの再取得要求がキー操作手段を介して入力されると、固有情報に含まれるアクセス情報を用いて複製元のデータ端末装置からコンテンツデータを再取得し、表示手段は、複製元に対応する情報を表示する。

【００２３】したがって、この発明によれば、ユーザは、自己のデータ端末装置の表示画面において複製したいコンテンツデータを選択するだけでコンテンツデータを自動的に複製できる。

【００２４】好ましくは、データ端末装置は、指示を入力するためのキー操作手段と、各種の情報を視覚情報としてユーザに表示する表示手段とをさらに備え、情報管理手段は、複製元のデータ端末装置から受信したコンテンツデータの個数に応じた複数の複製元に関する情報を管理し、制御手段は、キー操作手段を介して入力された複製元に関する情報の表示要求に応じて、情報管理手段から複数の複製元に関する情報を読出して表示手段に与え、表示手段によって表示された複数の複製元に関する情報のうちユーザによって選択された複製元に関する情報に含まれる付加情報に対応するコンテンツデータの再取得要求がキー操作手段を介して入力されると、固有情報に含まれるアクセス情報を用いて選択されたコンテンツデータの複製元のデータ端末装置からコンテンツデータを再取得し、表示手段は、複数の複製元に対応する情報を表示する。

【００２５】したがって、この発明によれば、ユーザは、以前に複製した複数のコンテンツデータから、再度、複製したいコンテンツデータを選択し、かつ、その選択したコンテンツデータを自動的に複製できる。

【００２６】好ましくは、制御手段は、複製元のデータ端末装置がコンテンツデータの複製に応じたとき、送受信手段を介して複製元のデータ端末装置からコンテンツデータを再取得する。

【００２７】したがって、この発明によれば、コンテンツデータの不正な複製を防止できる。

【００２８】好ましくは、コンテンツデータは、ライセンス鍵によって暗号化された暗号化コンテンツデータであり、制御手段は、キー操作手段を介して入力されたライセンス鍵を含むライセンスの配信要求に応じて、ライセンスを保持するサーバへアクセスし、サーバからライセンスを受信する。

【００２９】したがって、この発明によれば、著作権を保護しながら、コンテンツデータの複製を促進できる。

【００３０】また、この発明によれば、データ再取得方法は、複製されたコンテンツデータとコンテンツデータの付加情報とコンテンツデータの複製元の固有情報とを含むデータを受信し、付加情報および固有情報をコンテンツデータの複製元に関する情報として管理するデータ端末装置においてコンテンツデータを複製元のデータ端末装置から再取得するデータ再取得方法であって、受信した複製元に関する情報を表示手段に表示する第１のステップと、表示された複製元に関する情報に含まれる付加情報に対応するコンテンツデータの再取得要求を受付ける第２のステップと、表示された複製元に関する情報に含まれる固有情報に基づいて再取得要求がなされたコンテンツデータの複製元にアクセスし、複製元のデータ端末装置から複製されたコンテンツデータを再取得する第３のステップとを含む。

【００３１】したがって、この発明によれば、複製元の固有情報に基づいてコンテンツデータを複製元から容易に再取得できる。

【００３２】また、この発明によれば、データ再取得方法は、複製されたコンテンツデータおよびコンテンツデータの付加情報を含むデータと、コンテンツデータの複製元にアクセスするアクセス情報とを受信し、付加情報と受信したアクセス情報を用いて生成された前記複製元の固有情報とを前記複製元に関する情報として管理するデータ端末装置においてコンテンツデータを複製元のデータ端末装置から再取得するデータ再取得方法であって、受信した複製元に関する情報を表示手段に表示する

第１のステップと、表示された複製元に関する情報に含まれる付加情報に対応するコンテンツデータの再取得要求を受付ける第２のステップと、表示された複製元に関する情報に含まれる固有情報に基づいて再取得要求がなされたコンテンツデータの複製元にアクセスし、複製元のデータ端末装置から複製されたコンテンツデータを再取得する第３のステップとを含む。

【００３３】したがって、この発明によれば、複製元の固有情報として複製元のアクセス情報のみを受信する場合においても、複製元の固有情報に基づいてコンテンツデータを複製元から容易に再取得できる。

【００３４】好ましくは、第１のステップにおいて、複製元のデータ端末装置から受信したコンテンツデータの個数に応じた複数の複製元に関する情報を表示し、第２のステップにおいて、表示された複数の複製元に関する情報のうちユーザによって選択された複製元に関する情報に含まれる付加情報に対応するコンテンツデータの再取得要求が受付けられる。

【００３５】したがって、この発明によれば、以前の複製した複数のコンテンツデータから、再度、複製したいコンテンツデータを選択し、かつ、その選択したコンテンツデータを自動的に再複製できる。

【００３６】好ましくは、第３のステップにおいて、複製元のデータ端末装置がコンテンツデータの複製を許可したとき、複製元のデータ端末装置からコンテンツデータを再取得する。

【００３７】したがって、この発明によれば、コンテンツデータの不正な複製を防止できる。

【００３８】好ましくは、コンテンツデータは、ライセンス鍵によって暗号化された暗号化コンテンツデータであり、ライセンス鍵を含むライセンスの配信要求を受付ける第４のステップと、ライセンスを保持するサーバへアクセスし、サーバからライセンスを受信する第５のステップとをさらに含む。

【００３９】したがって、この発明によれば、著作権を保護しながら、コンテンツデータの複製を促進できる。

【００４０】

【発明の実施の形態】本発明の実施の形態について図面を参照しながら詳細に説明する。なお、図中同一または相当部分には同一符号を付してその説明は繰返さない。

【００４１】図１は、本発明の実施の形態によるデータ端末装置へ暗号化コンテンツデータを配信するデータ配信システムの全体構成を概念的に説明するための概略図である。

【００４２】なお、以下では携帯電話網を介してデジタル音楽データをユーザの携帯電話機１００，１０２，１０４，１０６に装着されたメモリカード１１０，１１２，１１４，１１６に配信するデータ配信システムの構成を例にとって説明するが、以下の説明で明らかとなるように、本発明はこのような場合に限定されることなく、他の著作物としてのコンテンツデータ、たとえば画像データ、動画像データ等を配信する場合においても適用することが可能なものである。

【００４３】図１を参照して、配信キャリア２０は、自己の携帯電話網を通じて得た、ユーザからの配信要求（配信リクエスト）を配信サーバ１０に中継する。著作権の存在する音楽データを管理する配信サーバ１０は、データ配信を求めてアクセスして来た携帯電話ユーザの携帯電話機１００，１０２，１０４，１０６に装着されたメモリカード１１０，１１２，１１４，１１６が正当な認証データを持つか否か、すなわち、正規のメモリカードであるか否かの認証処理を行ない、正当なメモリカードに対して所定の暗号方式により音楽データ（以下コンテンツデータとも呼ぶ）を暗号化した上で、データを配信するための配信キャリア２０である携帯電話会社に、このような暗号化コンテンツデータおよび暗号化コンテンツデータを再生するために必要な情報として暗号化コンテンツデータを復号するためのライセンス鍵を含むライセンスを与える。

【００４４】配信キャリア２０は、自己の携帯電話網を通じて配信要求を送信した携帯電話機１００，１０２，１０４，１０６に装着されたメモリカード１１０，１１２，１１４，１１６に対して、携帯電話網および携帯電話機１００，１０２，１０４，１０６を介して暗号化コンテンツデータとライセンスとを配信する。

【００４５】図１においては、たとえば携帯電話ユーザの携帯電話機１００，１０２，１０４，１０６には、それぞれ、着脱可能なメモリカード１１０，１１２，１１４，１１６が装着される構成となっている。メモリカード１１０，１１２，１１４，１１６は、それぞれ、携帯電話機１００，１０２，１０４，１０６により受信された暗号化コンテンツデータを受取り、上記配信にあたって行なわれた暗号化を復号した上で、携帯電話機１００，１０２，１０４，１０６中の音楽再生部（図示せず）に与える。

【００４６】さらに、たとえば携帯電話ユーザは、携帯電話機１００に接続したヘッドホーン１３０等を介してこのようなコンテンツデータを「再生」して、聴取することが可能である。図１においては、携帯電話機１０２，１０４，１０６へのヘッドホーンの接続を省略してあるが、携帯電話機１０２，１０４，１０６においてもヘッドホーンを介して再生したコンテンツデータを聴取できる。

【００４７】このような構成とすることで、まず、メモリカード１１０，１１２，１１４，１１６を利用しないと、配信サーバ１０からコンテンツデータの配信を受けて、音楽を再生することが困難な構成となる。

【００４８】しかも、配信キャリア２０において、たとえば１曲分のコンテンツデータを配信するたびにその度数を計数しておくことで、携帯電話ユーザがコンテンツ

データを受信（ダウンロード）するたびに発生する著作権料を、配信キャリア２０が携帯電話機の通話料とともに徴収することとすれば、著作権者が著作権料を確保することが容易となる。

【００４９】また、図１においては、配信サーバ１０から配信キャリア２０を介して携帯電話機１００，１０２，１０４，１０６へ配信された暗号化コンテンツデータの複製が、複数の携帯電話機１００，１０２，１０４，１０６の間で行なわれ、その複製された暗号化コンテンツデータを受信した携帯電話機１００（または１０２，１０４，１０６）は、受信した暗号化コンテンツデータを装着されたメモリカード１１０（または１１２，１１４，１１６）に格納するとともに、受信した暗号化コンテンツデータに付加された複製元の固有情報を保持する。そして、携帯電話機１００（または１０２，１０４，１０６）は、複製された暗号化コンテンツデータを削除した場合、または受信した暗号化コンテンツデータを記録したメモリカード１１０（１１２，１１４，１１６）がない場合に、複製された暗号化コンテンツデータが必要になったとき、自己が保持する複製元の固有情報に基づいて複製元の携帯電話機からコンテンツデータを再取得する。

【００５０】図１に示したような構成においては、暗号化して配信されるコンテンツデータを携帯電話機のユーザ側で再生可能とするためにシステム上必要とされるのは、第１には、通信における暗号鍵を配信するための方式であり、さらに第２には、配信したいコンテンツデータを暗号化する方式そのものであり、さらに、第３には、このように配信されたコンテンツデータの無断コピーを防止するためのコンテンツデータの保護を実現する構成である。

【００５１】本発明の実施の形態においては、特に、配信、および再生の各セッションの発生時において、これらのコンテンツデータの移動先に対する認証およびチェック機能を充実させ、非認証もしくは復号鍵の破られた記録装置およびデータ再生端末（コンテンツを再生できるデータ再生端末を携帯電話機とも言う。以下同じ）に対するコンテンツデータの出力を防止することによってコンテンツデータの著作権保護を強化する構成を説明する。

【００５２】なお、以下の説明においては、配信サーバ１０から、各携帯電話機にコンテンツデータを伝送する処理を「配信」と称することとする。

【００５３】図２は、図１に示したデータ配信システムにおいて、使用される通信のためのデータ、情報等の特性を説明する図である。

【００５４】まず、配信サーバ１０より配信されるデータについて説明する。Ｄｃは、音楽データ等のコンテンツデータである。コンテンツデータＤｃは、ライセンス鍵Ｋｃで復号可能な暗号化が施される。ライセンス鍵Ｋｃによって復号可能な暗号化が施された暗号化コンテンツデータ｛Ｄｃ｝Ｋｃがこの形式で配信サーバ１０より携帯電話機１００，１０２，１０４，１０６のユーザに配布される。

【００５５】なお、以下においては、｛Ｙ｝Ｘという表記は、データＹを、復号鍵Ｘにより復号可能な暗号化を施したことを示すものとする。

【００５６】さらに、配信サーバ１０からは、暗号化コンテンツデータとともに、コンテンツデータに関する著作権あるいはサーバアクセス関連等の平文情報としての付加情報Ｄｃ－ｉｎｆが配布される。また、ライセンスとして、ライセンス鍵Ｋｃ、配信サーバ１０からのライセンス鍵等の配信を特定するための管理コードであるトランザクションＩＤが配信サーバ１０と携帯電話機１００，１０２，１０４，１０６との間でやり取りされる。

【００５７】さらに、ライセンスとしては、コンテンツデータＤｃを識別するためのコードであるコンテンツＩＤや、利用者側からの指定によって決定されるライセンス数や機能限定等の情報を含んだライセンス購入条件ＡＣに基づいて生成される、記録装置（メモリカード）におけるライセンスのアクセスに対する制限に関する情報であるアクセス制御情報ＡＣｍおよびデータ再生端末における再生に関する制御情報である再生制御情報ＡＣｐ等が存在する。具体的には、アクセス制御情報ＡＣｍはメモリカードからライセンスまたはライセンス鍵を外部に出力するに当っての制御情報であり、再生可能回数（再生のためにライセンス鍵を出力する回数）、ライセンスの移動・複製に関する制限情報およびライセンスのセキュリティレベルなどがある。再生制御情報ＡＣｐは、再生するためにコンテンツ再生回路がライセンス鍵を受取った後に、再生を制限する情報であり、再生期限、再生速度変更制限、再生範囲指定（部分ライセンス）などがある。

【００５８】以後、トランザクションＩＤとコンテンツＩＤとを併せてライセンスＩＤと総称し、ライセンス鍵ＫｃとライセンスＩＤとアクセス制御情報ＡＣｍと再生制御情報ＡＣｐとを併せて、ライセンスと総称することとする。

【００５９】また、以降では、簡単化のためアクセス制御情報ＡＣｍは再生回数の制限を行なう制御情報である再生回数（０：再生不可、１～２５４：再生可能回数、２５５：制限無し）、ライセンスの移動および複製を制限する移動・複製フラグ（０：移動複製禁止、１：移動のみ可、２：移動複製可）の２項目とし、再生制御情報ＡＣｐは再生可能な期限を規定する制御情報である再生期限（ＵＴＣｔｉｍｅコード）のみを制限するものとする。

【００６０】本発明の実施の形態においては、記録装置（メモリカード）やコンテンツデータを再生する携帯電話機のクラスごとに、コンテンツデータの配信、および

再生を禁止することができるように禁止クラスリストＣＲＬ（Ｃｌａｓｓ Ｒｅｖｏｃａｔｉｏｎ Ｌｉｓｔ）の運用を行なう。以下では、必要に応じて記号ＣＲＬによって禁止クラスリスト内のデータを表わすこともある。

【００６１】禁止クラスリスト関連情報には、ライセンスの配信、および再生が禁止される携帯電話機、およびメモリカードのクラスをリストアップした禁止クラスリストデータＣＲＬが含まれる。コンテンツデータの保護にかかわるライセンスの管理・蓄積および再生を行なう全ての機器およびプログラムがリストアップの対象となる。

【００６２】禁止クラスリストデータＣＲＬは、配信サーバ１０内で管理されるとともに、メモリカード内にも記録保持される。このような禁止クラスリストは、随時バージョンアップしデータを更新していく必要があるが、データの変更については、基本的には暗号化コンテンツデータおよび／またはライセンス鍵等のライセンスを配信する際に、携帯電話機から受取った禁止クラスリストの更新日時を判断し、所有する禁止クラスリストＣＲＬの更新日時と比較して更新されていないと判断されたとき、更新された禁止クラスリストを携帯電話機に配信する。また、禁止クラスリストの変更については、変更点のみを反映した差分データである差分ＣＲＬを配信サーバ１０側より発生して、これに応じてメモリカード内の禁止クラスリストＣＲＬに追加する構成とすることも可能である。また、メモカード内で管理される禁止クラスリストＣＲＬには更新日時ＣＲＬｄａｔｅも更新時に記録されているものとする。

【００６３】このように、禁止クラスリストＣＲＬを、配信サーバのみならずライセンスを記録して管理するメモリカードにおいても保持運用することによって、再生やライセンスの移動・複製などに際して、クラス固有すなわち、コンテンツ再生回路（携帯電話機および再生端末）の種類に固有の復号鍵が破られた、コンテンツ再生回路（携帯電話機および再生端末）へのライセンス鍵あるいはライセンスの供給を禁止する。このため、携帯電話機ではコンテンツデータの再生が、メモリカードではライセンスの取得が行なえなくなり、新たなコンテンツデータを受信することができなくなる。

【００６４】このように、メモリカード内の禁止クラスリストＣＲＬは配信時に逐次データを更新する構成とする。また、メモリカード内における禁止クラスリストＣＲＬの管理は、上位レベルとは独立にメモリカード内では、ハード的に機密性を保証する高いレベルの耐タンパモジュール（Ｔａｍｐｅｒ Ｒｅｓｉｓｔａｎｔ Ｍｏｄｕｌｅ）に記録する。

【００６５】図３は、図１に示すデータ配信システムにおいて使用される通信のためのデータ、情報等の特性を説明する図である。

【００６６】コンテンツ再生回路、およびメモリカードには固有の公開暗号鍵ＫＰｐｙおよびＫＰｍｗがそれぞれ設けられ、公開暗号鍵ＫＰｐｙおよびＫＰｍｗはコンテンツ再生回路に固有の秘密復号鍵Ｋｐｙおよびメモリカードに固有の秘密復号鍵Ｋｍｗによってそれぞれ復号可能である。これら公開暗号鍵および秘密復号鍵は、コンテンツ再生デバイス、およびメモリカードの種類ごとに異なる値を持つ。これらの公開暗号鍵および秘密復号鍵を総称してクラス鍵と称し、これらの公開暗号鍵をクラス公開暗号鍵、秘密復号鍵をクラス秘密復号鍵、クラス鍵を共有する単位をクラスと称する。クラスは、製造会社や製品の種類、製造時のロット等によって異なる。

【００６７】また、コンテンツ再生回路（携帯電話機、再生端末）のクラス証明書としてＣｐｙが設けられ、メモリカードのクラス証明書としてＣｍｗが設けられる。これらのクラス証明書は、コンテンツ再生回路、およびメモリカードのクラスごとに異なる情報を有する。耐タンパモジュールが破られたり、クラス鍵による暗号が破られた、すなわち、秘密復号鍵が漏洩したクラスに対しては、禁止クラスリストにリストアップされてライセンス取得の禁止対象となる。

【００６８】これらのコンテンツ再生回路のクラス公開暗号鍵およびクラス証明書は、認証データ｛ＫＰｐｙ／／Ｃｐｙ｝ＫＰａの形式で、メモリカードのクラス公開暗号鍵およびクラス証明書は認証データ｛ＫＰｍｗ／／Ｃｍｗ｝ＫＰａの形式で、出荷時にデータ再生回路、およびメモリカードにそれぞれ記録される。後ほど詳細に説明するが、ＫＰａは配信システム全体で共通の公開認証鍵である。

【００６９】また、メモリカード１１０，１１２，１１４，１１６内のデータ処理を管理するための鍵として、メモリカードという媒体ごとに設定される公開暗号鍵ＫＰｍｃｘと、公開暗号鍵ＫＰｍｃｘで暗号化されたデータを復号することが可能なそれぞれに固有の秘密復号鍵Ｋｍｃｘが存在する。このメモリカードごとに個別な公開暗号鍵および秘密復号鍵を総称して個別鍵と称し、公開暗号鍵ＫＰｍｃｘを個別公開暗号鍵、秘密復号鍵Ｋｍｃｘを個別秘密復号鍵と称する。

【００７０】メモリカード外とメモリカード間でのデータ授受における秘密保持のための暗号鍵として、コンテンツデータの配信、および再生が行なわれるごとに配信サーバ１０、携帯電話機１００，１０２，１０４，１０６、メモリカード１１０，１１２，１１４，１１６において生成される共通鍵Ｋｓ１～Ｋｓ３が用いられる。

【００７１】ここで、共通鍵Ｋｓ１～Ｋｓ３は、配信サーバ、コンテンツ再生回路もしくはメモリカード間の通信の単位あるいはアクセスの単位である「セッション」ごとに発生する固有の共通鍵であり、以下においてはこれらの共通鍵Ｋｓ１～Ｋｓ３を「セッションキー」とも呼ぶこととする。

【００７２】これらのセッションキーＫｓ１～Ｋｓ３は、各セッションごとに固有の値を有することにより、配信サーバ、コンテンツ再生回路、およびメモリカードによって管理される。具体的には、セッションキーＫｓ１は、配信サーバによって配信セッションごとに発生される。セッションキーＫｓ２は、メモリカードによって配信セッションおよび再生セッションごとに発生し、セッションキーＫｓ３は、コンテンツ再生回路において再生セッションごとに発生される。各セッションにおいて、これらのセッションキーを授受し、他の機器で生成されたセッションキーを受けて、このセッションキーによる暗号化を実行した上でライセンス鍵等の送信を行なうことによって、セッションにおけるセキュリティ強度を向上させることができる。

【００７３】図４は、図１に示した配信サーバ１０の構成を示す概略ブロック図である。配信サーバ１０は、コンテンツデータを所定の方式に従って暗号化したデータやコンテンツＩＤ等の配信情報を保持するための情報データベース３０４と、携帯電話機の各ユーザごとにコンテンツデータへのアクセス開始に従った課金情報を保持するための課金データベース３０２と、禁止クラスリストＣＲＬを管理するＣＲＬデータベース３０６と、情報データベース３０４に保持されたコンテンツデータのメニューを保持するメニューデータベース３０７と、ライセンスの配信ごとにコンテンツデータおよびライセンス鍵等の配信を特定するトランザクションＩＤ等の配信に関するログを保持する配信記録データベース３０８と、情報データベース３０４、課金データベース３０２、ＣＲＬデータベース３０６、メニューデータベース３０７、および配信記録データベース３０８からのデータをバスＢＳ１を介して受取り、所定の処理を行なうためのデータ処理部３１０と、通信網を介して、配信キャリア２０とデータ処理部３１０との間でデータ授受を行なうための通信装置３５０とを備える。

【００７４】データ処理部３１０は、バスＢＳ１上のデータに応じて、データ処理部３１０の動作を制御するための配信制御部３１５と、配信制御部３１５に制御されて、配信セッション時にセッションキーＫｓ１を発生するためのセッションキー発生部３１６と、メモリカードから送られてきた認証のための認証データ｛ＫＰｍｗ／／Ｃｍｗ｝ＫＰａを復号するための公開認証鍵ＫＰａを保持する認証鍵保持部３１３と、メモリカードから送られてきた認証のための認証データ｛ＫＰｍｗ／／Ｃｍｗ｝ＫＰａを通信装置３５０およびバスＢＳ１を介して受けて、認証鍵保持部３１３からの公開認証鍵ＫＰａによって復号処理を行なう復号処理部３１２と、配信セッションごとに、セッション鍵Ｋｓ１を発生するセッションキー発生部３１６、セッションキー発生部３１６より生成されたセッションキーＫｓ１を復号処理部３１２によって得られたクラス公開暗号鍵ＫＰｍｗを用いて暗号化して、バスＢＳ１に出力するための暗号化処理部３１８と、セッションキーＫｓ１によって暗号化された上で送信されたデータをバスＢＳ１より受けて、復号処理を行なう復号処理部３２０とを含む。

【００７５】データ処理部３１０は、さらに、配信制御部３１５から与えられるライセンス鍵Ｋｃおよびアクセス制御情報ＡＣｍを、復号処理部３２０によって得られたメモリカードごとに固有の公開暗号鍵ＫＰｍｃｘによって暗号化するための暗号化処理部３２６と、暗号化処理部３２６の出力を、復号処理部３２０から与えられるセッションキーＫｓ２によってさらに暗号化してバスＢＳ１に出力するための暗号化処理部３２８とを含む。

【００７６】配信サーバ１０の配信セッションにおける動作については、後ほどフローチャートを使用して詳細に説明する。

【００７７】図５は、図１に示した携帯電話機１００，１０２，１０４，１０６の構成を説明するための概略ブロック図である。

【００７８】携帯電話機１００，１０２，１０４，１０６は、携帯電話網により無線伝送される信号を受信するアンテナ１１００と、アンテナ１１００からの信号を受けてベースバンド信号に変換、あるいは携帯電話機１００，１０２，１０４，１０６からのデータを変調してアンテナ１１００に与える送受信部１１０２と、携帯電話機１００，１０２，１０４，１０６の各部のデータ授受を行なうバスＢＳ２とを含む。

【００７９】携帯電話機１００，１０２，１０４，１０６は、さらに、携帯電話機１００，１０２，１０４，１０６のユーザの音声データを取込み、音声データをＡＤ変換部１１０６へ出力するマイク１１０４と、音声データをアナログ信号からデジタル信号に変換するＡＤ変換部１１０６と、デジタル信号に変換された音声信号を所定の方式に符号化する音声符号化部１１０８とを含む。

【００８０】携帯電話機１００，１０２，１０４，１０６は、さらに、他の携帯電話機から受信した音声信号を復号する音声再生部１１１０と、音声再生部１１１０からの音声信号をデジタル信号からアナログ信号に変換して音声データを出力するＤＡ変換部１１１２と、音声データを外部へ出力するスピーカ１１１４とを含む。

【００８１】携帯電話機１００，１０２，１０４，１０６は、さらに、外部からの指示を携帯電話機１００，１０２，１０４，１０６に与えるための操作パネル１１１６と、コントローラ１１２０等から出力される情報をユーザに視覚情報として与えるための表示パネル１１１８と、情報取得部１１２１により取得された暗号化コンテンツデータの付加情報および複製元の個人情報を記憶するメモリ１１１９と、バスＢＳ２を介して携帯電話機１００，１０２，１０４，１０６の動作を制御するためのコントローラ１１２０と、複製された暗号化コンテンツデータを受信した際に、その受信した暗号化コンテンツ

データに付加された付加情報および複製元の個人情報を取得する情報取得部１１２１とを含む。

【００８２】携帯電話機１００，１０２，１０４，１０６は、さらに、配信サーバ１０からのコンテンツデータ（音楽データ）を記憶し、かつ、復号処理を行なうための着脱可能なメモリカード１１０，１１２，１１４，１１６と、メモリカード１１０，１１２，１１４，１１６とバスＢＳ２との間のデータの授受を制御するためのメモリカードインタフェース１２００とを含む。

【００８３】携帯電話機１００，１０２，１０４，１０６は、さらに、クラス公開暗号鍵ＫＰｐ１およびクラス証明書Ｃｐ１を公開認証鍵ＫＰａで復号することでその正当性を認証できる状態に暗号化した認証データ｛ＫＰｐ１／／Ｃｐ１｝ＫＰａを保持する認証データ保持部１５００を含む。ここで、携帯電話機１００のクラスｙは、ｙ＝１であるとする。

【００８４】携帯電話機１００，１０２，１０４，１０６は、さらに、クラス固有の復号鍵であるＫｐ１を保持するＫｐ１保持部１５０２と、バスＢＳ２から受けたデータをＫｐ１によって復号し、メモリカード１１０，１１２，１１４，１１６によって発生されたセッションキーＫｓ２を得る復号処理部１５０４とを含む。

【００８５】携帯電話機１００，１０２，１０４，１０６は、さらに、メモリカード１１０，１１２，１１４，１１６に記憶されたコンテンツデータの再生を行なう再生セッションにおいてメモリカード１１０，１１２，１１４，１１６との間でバスＢＳ２上においてやり取りされるデータを暗号化するためのセッションキーＫｓ３を乱数等により発生するセッションキー発生部１５０８と、暗号化コンテンツデータの再生セッションにおいてメモリカード１１０，１１２，１１４，１１６からライセンス鍵Ｋｃおよび再生制御情報ＡＣｐを受取る際に、セッションキー発生部１５０８により発生されたセッションキーＫｓ３を復号処理部１５０４によって得られたセッションキーＫｓ２によって暗号化し、バスＢＳ３に出力する暗号化処理部１５０６とを含む。

【００８６】携帯電話機１００，１０２，１０４，１０６は、さらに、バスＢＳ２上のデータをセッションキーＫｓ３によって復号して、ライセンス鍵Ｋｃおよび再生制御情報ＡＣｐを出力する復号処理部１５１０と、バスＢＳ２より暗号化コンテンツデータ｛Ｄｃ｝Ｋｃを受けて、復号処理部１５１０より取得したライセンス鍵Ｋｃによって復号し、コンテンツデータを出力する復号処理部１５１６と、復号処理部１５１６の出力を受けてコンテンツデータを再生するための音楽再生部１５１８と、音楽再生部１５１８の出力をディジタル信号からアナログ信号に変換するＤＡ変換器１５１９と、ＤＡ変換器１５１９の出力をヘッドホーンなどの外部出力装置（図示省略）へ出力するための端子１５３０とを含む。

【００８７】なお、図５においては、点線で囲んだ領域は暗号化コンテンツデータを復号して音楽データを再生するコンテンツ再生デバイス１５５０を構成する。

【００８８】携帯電話機１００，１０２，１０４，１０６の各構成部分の各セッションにおける動作については、後ほどフローチャートを使用して詳細に説明する。

【００８９】図６は、図１に示すメモリカード１１０の構成を説明するための概略ブロック図である。

【００９０】既に説明したように、メモリカードのクラス公開暗号鍵およびクラス秘密復号鍵として、ＫＰｍｗおよびＫｍｗが設けられ、メモリカードのクラス証明書Ｃｍｗが設けられるが、メモリカード１１０においては、自然数ｗ＝３で表わされるものとする。また、メモリカードを識別する自然数ｘはｘ＝４で表されるものとする。

【００９１】したがって、メモリカード１１０は、認証データ｛ＫＰｍ３／／Ｃｍ３｝ＫＰａを保持する認証データ保持部１４００と、メモリカードごとに設定される固有の復号鍵である個別秘密復号鍵Ｋｍｃ４を保持するＫｍｃ保持部１４０２と、クラス秘密復号鍵Ｋｍ３を保持するＫｍ保持部１４２１と、個別秘密復号鍵Ｋｍｃ４によって復号可能な公開暗号鍵ＫＰｍｃ４を保持するＫＰｍｃ保持部１４１６とを含む。

【００９２】このように、メモリカードという記録装置の暗号鍵を設けることによって、以下の説明で明らかになるように、配信されたコンテンツデータや暗号化されたライセンス鍵の管理をメモリカード単位で実行することが可能になる。

【００９３】メモリカード１１０は、さらに、メモリインタフェース１２００との間で信号を端子１４２６を介して授受するインタフェース１４２４と、インタフェース１４２４との間で信号をやり取りするバスＢＳ３と、バスＢＳ３にインタフェース１４２４から与えられるデータから、クラス秘密復号鍵Ｋｍ３をＫｍ保持部１４２１から受けて、配信サーバ１０が配信セッションにおいて生成したセッションキーＫｓ１を接点Ｐａに出力する復号処理部１４２２と、ＫＰａ保持部１４１４から公開認証鍵ＫＰａを受けて、バスＢＳ３に与えられるデータから公開認証鍵ＫＰａによる復号処理を実行して復号結果と得られたクラス証明書をコントローラ１４２０に、得られたクラス公開鍵を暗号化処理部１４１０に出力する復号処理部１４０８と、切換スイッチ１４４２によって選択的に与えられる鍵によって、切換スイッチ１４４６によって選択的に与えられるデータを暗号化してバスＢＳ３に出力する暗号化処理部１４０６とを含む。

【００９４】メモリカード１１０は、さらに、配信、および再生の各セッションにおいてセッションキーＫｓ２を発生するセッションキー発生部１４１８と、セッションキー発生部１４１８の出力したセッションキーＫｓ２を復号処理部１４０８によって得られるクラス公開暗号鍵ＫＰｐｙもしくはＫＰｍｗによって暗号化してバスＢ

Ｓ３に送出する暗号化処理部１４１０と、バスＢＳ４よりセッションキーＫｓ２によって暗号化されたデータを受けてセッションキー発生部１４１８より得たセッションキーＫｓ２によって復号する復号処理部１４１２と、暗号化コンテンツデータの再生セッションにおいてメモリ１４１５から読出されたライセンス鍵Ｋｃおよび再生制御情報ＡＣｐを、復号処理部１４１２で復号された他のメモリカード１１０の個別公開暗号鍵ＫＰｍｃｘ（≠４）で暗号化する暗号処理部１４１７とを含む。

【００９５】メモリカード１１０は、さらに、バスＢＳ３上のデータを個別公開暗号鍵ＫＰｍｃ４と対をなすメモリカード１１０の個別秘密復号鍵Ｋｍｃ４によって復号するための復号処理部１４０４と、禁止クラスリストのバージョン更新のためのデータＣＲＬ＿ｄａｔによって逐次更新される禁止クラスリストデータＣＲＬと、暗号化コンテンツデータ｛Ｄｃ｝Ｋｃと、暗号化コンテンツデータ｛Ｄｃ｝Ｋｃを再生するためのライセンス（Ｋｃ，ＡＣｐ，ＡＣｍ，ライセンスＩＤ）と、付加情報Ｄａｔａ－ｉｎｆと、暗号化コンテンツデータの再生リストと、ライセンスを管理するためのライセンス管理ファイルとをバスＢＳ３より受けて格納するためのメモリ１４１５とを含む。メモリ１４１５は、例えば半導体メモリによって構成される。また、メモリ１５１５は、ＣＲＬ領域１４１５Ａと、ライセンス領域１４１５Ｂと、データ領域１４１５Ｃとから成る。ＣＲＬ領域１４１５Ａは、禁止クラスリストＣＲＬを記録するための領域である。ライセンス領域１４１５Ｂは、ライセンスを記録するための領域である。データ領域１４１５Ｃは、暗号化コンテンツデータ｛Ｄｃ｝Ｋｃ、暗号化コンテンツデータの関連情報Ｄｃ－ｉｎｆ、ライセンスを管理するために必要な情報を暗号化コンテンツごとに記録するライセンス管理ファイル、およびメモリカードに記録された暗号化コンテンツデータやライセンスにアクセスするための基本的な情報を記録する再生リストファイルを記録するための領域である。そして、データ領域１４１５Ｃは、外部から直接アクセスが可能である。ライセンス管理ファイルおよび再生リストファイルの詳細については後述する。

【００９６】ライセンス領域１４１５Ｂは、ライセンス（ライセンス鍵Ｋｃ、再生制御情報ＡＣｐ、アクセス制限情報ＡＣｍ、ライセンスＩＤ）を記録するためにエントリと呼ばれるライセンス専用の記録単位でライセンスを格納する。ライセンスに対してアクセスする場合には、ライセンスか格納されている、あるいは、ライセンスを記録したいエントリをエントリ番号によって指定する構成になっている。

【００９７】メモリカード１１０は、さらに、バスＢＳ３を介して外部との間でデータ授受を行ない、バスＢＳ３との間で再生情報等を受けて、メモリカード１１０の動作を制御するためのコントローラ１４２０を含む。

【００９８】なお、データ領域１４１５Ｃを除く全ての構成は、耐タンパモジュール領域に構成される。

【００９９】メモリカード１１２，１１４，１１６は、メモリカード１１０と同じ構成から成る。この場合、メモリカード１１２，１１４，１１６においては、自然数ｗは３以外の自然数が設定され、自然数ｘは４以外の自然数が設定される。

【０１００】以下、図１に示すデータ配信システムにおける各セッションの動作について説明する。

【０１０１】［配信１］まず、図１に示すデータ配信システムにおいて、配信サーバ１０から携帯電話機１００に装着されたメモリカード１１０へ暗号化コンテンツデータおよびライセンスを配信する動作について説明する。なお、この動作を「配信」という。

【０１０２】図７～図１０は、図１に示すデータ配信システムにおける暗号化コンテンツデータの購入時に発生する携帯電話機１００に装着されたメモリカード１１０への配信動作（以下、配信セッションともいう）を説明するための第１～第４のフローチャートである。

【０１０３】図７における処理以前に、携帯電話機１００のユーザは、配信サーバ１０に対して接続し、購入を希望するコンテンツに対するコンテンツＩＤを取得していることを前提としている。

【０１０４】図７を参照して、携帯電話機１００のユーザから操作パネル１１１６を介してコンテンツＩＤの指定による配信リクエストがなされる（ステップＳ１００）。そして、操作パネル１１１６を介して暗号化コンテンツデータのライセンスを購入するための購入条件ＡＣが入力される（ステップＳ１０２）。つまり、選択した暗号化コンテンツデータを復号するライセンス鍵Ｋｃを購入するために、暗号化コンテンツデータのアクセス制御情報ＡＣｍ、および再生制御情報ＡＣｐを設定して購入条件ＡＣが入力される。

【０１０５】暗号化コンテンツデータの購入条件ＡＣが入力されると、コントローラ１１２０は、バスＢＳ２およびメモリカードインタフェース１２００を介してメモリカード１１０へ認証データの出力指示を与える（ステップＳ１０４）。メモリカード１１０のコントローラ１４２０は、端子１４２６、インタフェース１４２４およびバスＢＳ３を介して認証データの出力指示を受取る。そして、コントローラ１４２０は、バスＢＳ３を介して認証データ保持部１４００から認証データ｛ＫＰｍ３／／Ｃｍ３｝ＫＰａを読出し、｛ＫＰｍ３／／Ｃｍ３｝ＫＰａをバスＢＳ３、インタフェース１４２４および端子１４２６を介して出力する（ステップＳ１０６）。

【０１０６】携帯電話機１００のコントローラ１１２０は、メモリカード１１０からの認証データ｛ＫＰｍ３／／Ｃｍ３｝ＫＰａに加えて、コンテンツＩＤ、ライセンス購入条件のデータＡＣ、および配信リクエストを配信サーバ１０に対して送信する（ステップＳ１０８）。

【０１０７】配信サーバ１０では、携帯電話機１００から配信リクエスト、コンテンツＩＤ、認証データ｛ＫＰｍ３／／Ｃｍ３｝ＫＰａ、およびライセンス購入条件のデータＡＣを受信し（ステップＳ１１０）、復号処理部３１２においてメモリカード１１０から出力された認証データを公開認証鍵ＫＰａで復号処理を実行する（ステップＳ１１２）。

【０１０８】配信制御部３１５は、復号処理部３１２における復号処理結果から、正規の機関でその正当性を証明するための暗号化を施した認証データを受信したか否かを判断する認証処理を行なう（ステップＳ１１４）。正当な認証データであると判断された場合、配信制御部３１５は、クラス公開暗号鍵ＫＰｍ３およびクラス証明書Ｃｍ３を承認し、受理する。そして、次の処理（ステップＳ１１６）へ移行する。正当な認証データでない場合には、非承認とし、クラス公開暗号鍵ＫＰｍ３およびクラス証明書Ｃｍ３を受理しないで配信セッションを終了する（ステップＳ１９８）。

【０１０９】認証の結果、クラス公開暗号鍵ＫＰｍ３およびクラス証明書Ｃｍ３を受理すると、配信制御部３１５は、次に、メモリカード１１０のクラス証明書Ｃｍ３が禁止クラスリストＣＲＬにリストアップされているかどうかをＣＲＬデータベース３０６に照会し、これらのクラス証明書が禁止クラスリストの対象になっている場合には、ここで配信セッションを終了する（ステップＳ１９８）。

【０１１０】一方、メモリカード１１０のクラス証明書が禁止クラスリストの対象外である場合には次の処理に移行する（ステップＳ１１６）。

【０１１１】認証の結果、正当な認証データを持つメモリカードを備える携帯電話機からのアクセスであり、クラスが禁止クラスリストの対象外であることが確認されると、配信サーバ１０において、配信制御部３１５は、配信を特定するための管理コードであるトランザクションＩＤを生成する（ステップＳ１１８）。また、セッションキー発生部３１６は、配信のためのセッションキーＫｓ１を生成する（ステップＳ１２０）。セッションキーＫｓ１は、復号処理部３１２によって得られたメモリカード１１０に対応するクラス公開暗号鍵ＫＰｍ３によって、暗号化処理部３１８によって暗号化される（ステップＳ１２２）。

【０１１２】トランザクションＩＤおよび暗号化されたセッションキーＫｓ１は、トランザクションＩＤ／／｛Ｋｓ１｝Ｋｍ３として、バスＢＳ１および通信装置３５０を介して外部に出力される（ステップＳ１２４）。

【０１１３】図８を参照して、携帯電話機１００が、トランザクションＩＤ／／｛Ｋｓ１｝Ｋｍ３を受信すると（ステップＳ１２６）、コントローラ１１２０は、トランザクションＩＤ／／｛Ｋｓ１｝Ｋｍ３をメモリカード１１０に入力する（ステップＳ１２８）。そうすると、メモリカード１１０においては、端子１４２６およびインタフェース１４２４を介して、バスＢＳ３に与えられた受信データを、復号処理部１４２２が、保持部１４２１に保持されるメモリカード１１０に固有なクラス秘密復号鍵Ｋｍ３によって復号処理することにより、セッションキーＫｓ１を復号し、セッションキーＫｓ１を受理する（ステップＳ１３０）。

【０１１４】コントローラ１４２０は、配信サーバ１０で生成されたセッションキーＫｓ１の受理を確認すると、セッションキー発生部１４１８に対してメモリカード１１０において配信動作時に生成されるセッションキーＫｓ２の生成を指示する。そして、セッションキー発生部１４１８は、セッションキーＫｓ２を生成する（ステップＳ１３２）。

【０１１５】また、配信セッションにおいては、コントローラ１４２０は、メモリカード１１０内のメモリ１４１５に記録されている禁止クラスリストＣＲＬから更新日時ＣＲＬｄａｔｅを抽出して切換スイッチ１４４６に出力する（ステップＳ１３４）。

【０１１６】暗号処理部１４０６は、切換スイッチ１４４２の接点Ｐａを介して復号処理部１４２２より与えられるセッションキーＫｓ１によって、切換スイッチ１４４６の接点を順次切換えることによって与えられるセッションキーＫｓ２、個別公開暗号鍵ＫＰｍｃ４および禁止クラスリストの更新日時ＣＲＬｄａｔｅを１つのデータ列として暗号化して、｛Ｋｓ２／／ＫＰｍｃ４／／ＣＲＬｄａｔｅ｝Ｋｓ１をバスＢＳ３に出力する（ステップＳ１３６）。

【０１１７】バスＢＳ３に出力された暗号化データ｛Ｋｓ２／／ＫＰｍｃ４／／ＣＲＬｄａｔｅ｝Ｋｓ１は、バスＢＳ３からインタフェース１４２４および端子１４２６を介して携帯電話機１００に出力され、携帯電話機１００から配信サーバ１０に送信される（ステップＳ１３８）。

【０１１８】配信サーバ１０は、トランザクションＩＤ／／｛Ｋｓ２／／ＫＰｍｃ４／／ＣＲＬｄａｔｅ｝Ｋｓ１を受信して、復号処理部３２０においてセッションキーＫｓ１による復号処理を実行し、メモリカード１１０で生成されたセッションキーＫｓ２、メモリカード１１０に固有の公開暗号鍵ＫＰｍｃ４およびメモリカード１１０における禁止クラスリストＣＲＬの更新日時ＣＲＬｄａｔｅを受理する（ステップＳ１４２）。

【０１１９】配信制御部３１５は、ステップＳ１１０で取得したコンテンツＩＤおよびライセンス購入条件のデータＡＣに従って、アクセス制御情報ＡＣｍおよび再生制御情報ＡＣｐを生成する（ステップＳ１４４）。さらに、暗号化コンテンツデータを復号するためのライセンス鍵Ｋｃを情報データベース３０４より取得する（ステップＳ１４６）。

【０１２０】配信制御部３１５は、生成したライセン

ス、すなわち、トランザクションＩＤ、コンテンツＩＤ、ライセンス鍵Ｋｃ、再生制御情報ＡＣｐ、およびアクセス制御情報ＡＣｍを暗号化処理部３２６に与える。暗号化処理部３２６は、復号処理部３２０によって得られたメモリカード１１０に固有の公開暗号鍵ＫＰｍｃ４によってライセンスを暗号化して暗号化データ｛トランザクションＩＤ／／コンテンツＩＤ／／Ｋｃ／／ＡＣｍ／／ＡＣｐ｝Ｋｍｃ４を生成する（ステップＳ１４８）。

【０１２１】図９を参照して、配信サーバ１０において、メモリカード１１０から送信された禁止クラスリストの更新日時ＣＲＬｄａｔｅが、ＣＲＬデータベース３０６に保持される配信サーバ１０の禁止クラスリストＣＲＬの更新日時と比較されることによってメモリカード１１０が保持する禁止クラスリストＣＲＬが最新か否かが判断され、メモリカード１１０が保持する禁止クラスリストＣＲＬが最新と判断されたとき、ステップＳ１５２へ移行する。また、メモリカード１１０が保持する禁止クラスリストＣＲＬが最新でないときはステップＳ１６０へ移行する（ステップＳ１５０）。

【０１２２】最新と判断されたとき、暗号化処理部３２８は、暗号化処理部３２６から出力された暗号化データ｛トランザクションＩＤ／／コンテンツＩＤ／／Ｋｃ／／ＡＣｍ／／ＡＣｐ｝Ｋｍｃ４をメモリカード１１０において発生されたセッションキーＫｓ２によって暗号化を行ない、暗号化データ｛｛トランザクションＩＤ／／コンテンツＩＤ／／Ｋｃ／／ＡＣｍ／／ＡＣｐ｝Ｋｍｃ４｝Ｋｓ２をバスＢＳ１に出力する。そして、配信制御部３１５は、バスＢＳ１上の暗号化データ｛｛トランザクションＩＤ／／コンテンツＩＤ／／Ｋｃ／／ＡＣｍ／／ＡＣｐ｝Ｋｍｃ４｝Ｋｓ２を通信装置３５０を介して携帯電話機１００へ送信する（ステップＳ１５２）。

【０１２３】そして、携帯電話機１００のコントローラ１１２０は、暗号化データ｛｛トランザクションＩＤ／／コンテンツＩＤ／／Ｋｃ／／ＡＣｍ／／ＡＣｐ｝Ｋｍｃ４｝Ｋｓ２を受信し（ステップＳ１５４）、バスＢＳ２およびメモリカードインタフェース１２００を介してメモリカード１１０に入力する。メモリカード１１０の復号処理部１４１２は、暗号化データ｛｛トランザクションＩＤ／／コンテンツＩＤ／／Ｋｃ／／ＡＣｍ／／ＡＣｐ｝Ｋｍｃ４｝Ｋｓ２を端子１４２６およびインタフェース１４２４を介して受取り、セッションキー発生部１４１８によって発生されたセッションキーＫｓ２によって復号し、｛トランザクションＩＤ／／コンテンツＩＤ／／Ｋｃ／／ＡＣｍ／／ＡＣｐ｝Ｋｍｃ４を受理する（ステップＳ１５８）。その後、ステップＳ１７２へ移行する。

【０１２４】一方、配信サーバ１０において、メモリカード１１０が保持する禁止クラスリストＣＲＬが最新でないと判断されると、配信制御部３１５は、バスＢＳ１を介してＣＲＬデータベース３０６から最新の禁止クラスリストＣＲＬを取得し、差分データである差分ＣＲＬを生成する（ステップＳ１６０）。

【０１２５】暗号化処理部３２８は、暗号化処理部３２６の出力と、配信制御部３１５がバスＢＳ１を介して供給する禁止クラスリストの差分ＣＲＬとを受けて、メモリカード１１０において生成されたセッションキーＫｓ２によって暗号化する。暗号化処理部３２８より出力された暗号化データ｛差分ＣＲＬ／／｛トランザクションＩＤ／／コンテンツＩＤ／／Ｋｃ／／ＡＣｍ／／ＡＣｐ｝Ｋｍｃ４｝Ｋｓ２は、バスＢＳ１および通信装置３５０を介して携帯電話機１００に送信される（ステップＳ１６２）。

【０１２６】携帯電話機１００は、送信された暗号化データ｛差分ＣＲＬ／／｛トランザクションＩＤ／／コンテンツＩＤ／／Ｋｃ／／ＡＣｍ／／ＡＣｐ｝Ｋｍｃ４｝Ｋｓ２を受信し（ステップＳ１６４）、バスＢＳ２およびメモリカードインタフェース１２００を介してメモリカード１１０に入力する（ステップＳ１６６）。メモリカード１１０においては、端子１４２６およびインタフェース１４２４を介して、バスＢＳ３に与えられた受信データを復号処理部１４１２によって復号する。復号処理部１４１２は、セッションキー発生部１４１８から与えられたセッションキーＫｓ２を用いてバスＢＳ３上の受信データを復号しバスＢＳ３に出力する（ステップＳ１６８）。

【０１２７】この段階で、バスＢＳ３には、Ｋｍｃ保持部１４０２に保持される秘密復号鍵Ｋｍｃ４で復号可能な暗号化ライセンス｛トランザクションＩＤ／／コンテンツＩＤ／／Ｋｃ／／ＡＣｍ／／ＡＣｐ｝Ｋｍｃ４と、差分ＣＲＬとが出力される（ステップＳ１６８）。コントローラ１４２０の指示によって受理した差分ＣＲＬによってメモリ１４１５内のＣＲＬ領域１４１５Ａを差分ＣＲＬに基づいて更新する（ステップＳ１７０）。

【０１２８】ステップＳ１５２，Ｓ１５４，Ｓ１５６，Ｓ１５８は、メモリカード１１０の禁止クラスリストＣＲＬが最新の場合のライセンスのメモリカード１１０への配信動作であり、ステップＳ１６０，Ｓ１６２，Ｓ１６４，Ｓ１６６，Ｓ１６８，Ｓ１７０は、メモリカード１１０の禁止クラスリストＣＲＬが最新でない場合のライセンスのメモリカード１１０への配信動作である。このように、メモリカード１１０から送られてきた禁止クラスリストの更新日時ＣＲＬｄａｔｅによって、配信を求めてきたメモリカード１１０の禁止クラスリストＣＲＬが最新か否かを、逐一、確認し、最新でないとき、最新の禁止クラスリストＣＲＬをＣＲＬデータベース３０６から取得し、差分ＣＲＬをメモリカード１１０に配信することによって、ライセンスの破られたメモリカードへのライセンスの配信を防止できる。

【０１２９】ステップＳ１５８またはステップＳ１７０

の後、コントローラ１４２０の指示によって、暗号化ライセンス｛トランザクションＩＤ／／コンテンツＩＤ／／Ｋｃ／／ＡＣｍ／／ＡＣｐ｝Ｋｍｃ４は、復号処理部１４０４において、個別秘密復号鍵Ｋｍｃ４によって復号され、ライセンス（ライセンス鍵Ｋｃ、トランザクションＩＤ、コンテンツＩＤ、アクセス制御情報ＡＣｍおよび再生制御情報ＡＣｐ）が受理される（ステップＳ１７２）。

【０１３０】図１０を参照して、携帯電話機１００のコントローラ１１２０は、メモリカード１１０が受理したライセンスを格納するエントリを指示するためのエントリ番号を、メモリカード１１０に入力する（ステップＳ１７４）。そうすると、メモリカード１１０のコントローラ１４２０は、端子１４２６およびインタフェース１４２４を介してエントリ番号を受取り、その受取ったエントリ番号によって指定されるメモリ１４１５のライセンス領域１４１５Ｂに、ステップＳ１７２において取得したライセンス（ライセンス鍵Ｋｃ、トランザクションＩＤ、コンテンツＩＤ、アクセス制御情報ＡＣｍおよび再生制御情報ＡＣｐ）を格納する（ステップＳ１７６）。

【０１３１】そして、携帯電話機１００のコントローラ１１２０は、配信サーバ１０から送られたトランザクションＩＤと、暗号化コンテンツデータの配信要求を配信サーバ１０へ送信する（ステップＳ１７８）。

【０１３２】配信サーバ１０は、トランザクションＩＤおよび暗号化コンテンツデータの配信要求を受信し（ステップＳ１８０）、情報データベース３０４より、暗号化コンテンツデータ｛Ｄｃ｝Ｋｃおよび付加情報Ｄｃ－ｉｎｆを取得して、これらのデータをバスＢＳ１および通信装置３５０を介して出力する（ステップＳ１８２）。

【０１３３】携帯電話機１００は、｛Ｄｃ｝Ｋｃ／／Ｄｃ－ｉｎｆを受信して、暗号化コンテンツデータ｛Ｄｃ｝Ｋｃおよび付加情報Ｄｃ－ｉｎｆを受理する（ステップＳ１８４）。そうすると、携帯電話機１００のコントローラ１１２０は、暗号化コンテンツデータ｛Ｄｃ｝Ｋｃおよび付加情報Ｄｃ－ｉｎｆを１つのコンテンツファイルとしてバスＢＳ２およびメモリカードインタフェース１２００を介してメモリカード１１０へ入力する（ステップＳ１８６）。

【０１３４】そうすると、メモリカード１１０のコントローラ１４２０は、端子１４２６、インタフェース１４２４、およびバスＢＳ３を介して暗号化コンテンツデータ｛Ｄｃ｝Ｋｃおよび付加情報Ｄｃ－ｉｎｆを受取り、その受取った暗号化コンテンツデータ｛Ｄｃ｝Ｋｃおよび付加情報Ｄｃ－ｉｎｆをバスＢＳ３を介してメモリ１４１５のデータ領域１４１５Ｃに記録する（ステップＳ１８７）。また、コントローラ１４２０は、メモリカード１１０に格納されたライセンスのエントリ番号と、平文のトランザクションＩＤおよびコンテンツＩＤを含む暗号化コンテンツデータ｛Ｄｃ｝Ｋｃと付加情報Ｄｃ－ｉｎｆに対するライセンス管理ファイルを生成し、バスＢＳ３を介してメモリ１４１５のデータ領域１４１５Ｃに記録する（ステップＳ１８８）。さらに、コントローラ１４２０は、メモリ１４１５に記録されているコンテンツリストファイルに受理したコンテンツの情報として、記録したコンテンツファイル及びライセンス管理ファイルの名称や、付加情報Ｄｃ－ｉｎｆから抽出した暗号化コンテンツデータに関する情報（曲名、アーティスト名）等を追記する（ステップＳ１９０）。そして、携帯電話機１００のコントローラ１１２０は、トランザクションＩＤと配信受理を配信サーバ１０へ送信する（ステップＳ１９２）。

【０１３５】配信サーバ１０は、トランザクションＩＤ／／配信受理を受信すると（ステップＳ１９４）、課金データベース３０２への課金データの格納、およびトランザクションＩＤの配信記録データベース３０８への記録が行われて配信終了の処理が実行され（ステップＳ１９６）、全体の処理が終了する（ステップＳ１９８）。

【０１３６】このようにして、携帯電話機１００に装着されたメモリカード１１０が正規の認証データを保持する機器であること、同時に、クラス証明書Ｃｍ３とともに暗号化して送信できた公開暗号鍵ＫＰｍ３が有効であることを確認した上で、クラス証明書Ｃｍ３が禁止クラスリスト、すなわち、公開暗号鍵ＫＰｍ３による暗号化が破られたクラス証明書リストに記載されていないメモリカードからの配信要求に対してのみコンテンツデータを配信することができ、不正なメモリカードへの配信および解読されたクラス鍵を用いた配信を禁止することができる。

【０１３７】携帯電話機１０２に装着されたメモリカード１１２、携帯電話機１０４に装着されたメモリカード１１４、および携帯電話機１０６に装着されたメモリカード１１６への暗号化コンテンツデータの配信動作も図７～図１０に示すフローチャートに従って行なわれる。

【０１３８】［再生］次に、図１１および図１２を参照してメモリカード１１０に記録されたコンテンツデータの携帯電話機１００における再生動作について説明する。なお、図１１における処理以前に、携帯電話機１００のユーザは、メモリカード１１０のデータ領域１４１５Ｃに記録されている再生リストに従って、再生するコンテンツ（楽曲）を決定し、コンテンツファイルを特定し、ライセンス管理ファイルを取得していることを前提として説明する。

【０１３９】図１１を参照して、再生動作の開始とともに、携帯電話機１００のユーザから操作パネル１１１６を介して再生指示が携帯電話機１００にインプットされる（ステップＳ７００）。そうすると、コントローラ１１２０は、バスＢＳ２を介して認証データ保持部１５０

０から認証データ｛ＫＰｐ１／／Ｃｐ１｝ＫＰａを読出し、メモリカードインタフェース１２００を介してメモリカード１１０へ認証データ｛ＫＰｐ１／／Ｃｐ１｝ＫＰａを出力する（ステップＳ７０２）。

【０１４０】そうすると、メモリカード１１０は、認証データ｛ＫＰｐ１／／Ｃｐ１｝ＫＰａを受理する（ステップＳ７０４）。そして、メモリカード１１０の復号処理部１４０８は、受理した認証データ｛ＫＰｐ１／／Ｃｐ１｝ＫＰａを、ＫＰａ保持部１４１４に保持された公開認証鍵ＫＰａによって復号し（ステップＳ７０６）、コントローラ１４２０は復号処理部１４０８における復号処理結果から、認証処理を行なう。すなわち、認証データ｛ＫＰｐ１／／Ｃｐ１｝ＫＰａが正規の認証データであるか否かを判断する認証処理を行なう（ステップＳ７０８）。復号できなかった場合、ステップＳ７４８へ移行し、再生動作は終了する。認証データが復号できた場合、コントローラ１４２０は、取得した証明書Ｃｍ１がメモリ１４１５のＣＲＬ領域１４１５Ａから読出した禁止クラスリストＣＲＬに含まれるか否かを判断する（ステップＳ７１０）。この場合、クラス証明書Ｃｐ１には識別番号が付与されており、コントローラ１４２０は、受理したクラス証明書Ｃｐ１の識別番号が禁止クラスリストデータの中に存在するか否かを判別する。クラス証明書Ｃｐ１が禁止クラスリストデータに含まれると判断されると、ステップＳ７４８へ移行し、再生動作は終了する。

【０１４１】ステップＳ７１０において、クラス証明書Ｃｐ１が禁止クラスリストデータＣＲＬに含まれていないと判断されると、メモリカード１１０のセッションキー発生部１４１８は、再生セッション用のセッションキーＫｓ２を発生させる（ステップＳ７１２）。そして、暗号処理部１４１０は、セッションキー発生部１４１８からのセッションキーＫｓ２を、復号処理部１４０８で復号された公開暗号鍵ＫＰｐ１によって暗号化した｛Ｋｓ２｝Ｋｐ１をバスＢＳ３へ出力する（ステップＳ７１４）。そうすると、コントローラ１４２０は、インタフェース１４２４および端子１４２６を介してメモリカードインタフェース１２００へ｛Ｋｓ２｝Ｋｐ１を出力する（ステップＳ７１６）。携帯電話機１００のコントローラ１１２０は、メモリカードインタフェース１２００を介して｛Ｋｓ２｝Ｋｐ１を取得する。そして、Ｋｐ１保持部１５０２は、秘密復号鍵Ｋｐ１を復号処理部１５０４へ出力する。

【０１４２】復号処理部１５０４は、Ｋｐ１保持部１５０２から出力された、公開暗号鍵ＫＰｐ１と対になっている秘密復号鍵Ｋｐ１によって｛Ｋｓ２｝Ｋｐ１を復号し、セッションキーＫｓ２を暗号処理部１５０６へ出力する（ステップＳ７１８）。そうすると、セッションキー発生部１５０８は、再生セッション用のセッションキーＫｓ３を発生させ、セッションキーＫｓ３を暗号処理部１５０６へ出力する（ステップＳ７２０）。暗号処理部１５０６は、セッションキー発生部１５０８からのセッションキーＫｓ３を復号処理部１５０４からのセッションキーＫｓ２によって暗号化して｛Ｋｓ３｝Ｋｓ２を出力し、コントローラ１１２０は、バスＢＳ２およびメモリカードインタフェース１２００を介して｛Ｋｓ３｝Ｋｓ２をメモリカード１１０へ出力する（ステップＳ７２２）。

【０１４３】そうすると、メモリカード１１０の復号処理部１４１２は、端子１４２６、インタフェース１４２４、およびバスＢＳ３を介して｛Ｋｓ３｝Ｋｓ２を入力する（ステップＳ７２４）。

【０１４４】図１２を参照して、復号処理部１４１２は、セッションキー発生部１４１８によって発生されたセッションキーＫｓ２によって｛Ｋｓ３｝Ｋｓ２を復号して、携帯電話機１００で発生されたセッションキーＫｓ３を受理する（ステップＳ７２６）。

【０１４５】携帯電話機１００のコントローラ１１２０は、メモリカード１１０から事前に取得した再生リクエスト曲のライセンス管理ファイルからライセンスの格納されているエントリ番号を取得し、メモリカードインタフェース１２００を介してメモリカード１１０へ取得したエントリ番号を出力する（ステップＳ７２７）。

【０１４６】エントリ番号が入力に応じて、コントローラ１４２０は、アクセス制限情報ＡＣｍを確認する（ステップＳ７２８）。

【０１４７】ステップＳ７２８においては、メモリのアクセスに対する制限に関する情報であるアクセス制限情報ＡＣｍを確認することにより、具体的には、再生回数を確認することにより、既に再生不可の状態である場合には再生動作を終了し、アクセス制限情報の再生回数に制限がある場合にはアクセス制限情報ＡＣｍの再生回数を更新（１減ずる）した後に次のステップに進む（ステップＳ７３０）。一方、アクセス制限情報ＡＣｍの再生回数によって再生が制限されていない場合においては、ステップＳ７３０はスキップされ、アクセス制限情報ＡＣｍの再生回数は更新されることなく処理が次のステップ（ステップＳ７３２）に進行される。

【０１４８】ステップＳ７２８において、当該再生動作において再生が可能であると判断された場合には、メモリ１４１５のライセンス領域１４１５Ｂに記録された再生リクエスト曲のライセンス鍵Ｋｃおよび再生制御情報ＡＣｐがバスＢＳ３上に出力される（ステップＳ７３２）。

【０１４９】得られたライセンス鍵Ｋｃと再生制御情報ＡＣｐは、切換スイッチ１４４６の接点Ｐｆを介して暗号化処理部１４０６に送られる。暗号化処理部１４０６は、切換スイッチ１４４２の接点Ｐｂを介して復号処理部１４１２より受けたセッションキーＫｓ３によって切換スイッチ１４４６を介して受けたライセンス鍵Ｋｃと

再生制御情報ＡＣｐとを暗号化し、暗号化データ｛Ｋｃ／／ＡＣｐ｝Ｋｓ３をバスＢＳ３に出力する（ステップＳ７３４）。

【０１５０】バスＢＳ３に出力された暗号化データは、インタフェース１４２４、端子１４２６、およびメモリカードインタフェース１２００を介して携帯電話機１００に送出される。

【０１５１】携帯電話機１００においては、メモリカードインタフェース１２００を介してバスＢＳ２に伝達される暗号化データ｛Ｋｃ／／ＡＣｐ｝Ｋｓ３を復号処理部１５１０によって復号処理を行ない、ライセンス鍵Ｋｃおよび再生制御情報ＡＣｐを受理する（ステップＳ７３６）。復号処理部１５１０は、ライセンス鍵Ｋｃを復号処理部１５１６に伝達し、再生制御情報ＡＣｐをバスＢＳ２に出力する。

【０１５２】コントローラ１１２０は、バスＢＳ２を介して、再生制御情報ＡＣｐを受理して再生の可否の確認を行なう（ステップＳ７４０）。

【０１５３】ステップＳ７４０においては、再生制御情報ＡＣｐによって再生不可と判断される場合には、再生動作は終了される。

【０１５４】ステップＳ７４０において再生可能と判断された場合、コントローラ１１２０は、メモリカードインタフェース１２００を介してメモリカード１１０に暗号化コンテンツデータ｛Ｄｃ｝Ｋｃを要求する。そうすると、メモリカード１１０のコントローラ１４２０は、メモリ１４１５から暗号化コンテンツデータ｛Ｄｃ｝Ｋｃを取得し、バスＢＳ３、インタフェース１４２４、および端子１４２６を介してメモリカードインタフェース１２００へ出力する（ステップＳ７４２）。

【０１５５】携帯電話機１００のコントローラ１１２０は、メモリカードインタフェース１２００を介して暗号化コンテンツデータ｛Ｄｃ｝Ｋｃを取得し、バスＢＳ２を介して暗号化コンテンツデータ｛Ｄｃ｝Ｋｃを復号処理部１５１６へ与える。

【０１５６】そして、復号処理部１５１６は、暗号化コンテンツデータ｛Ｄｃ｝Ｋｃを復号処理部１５１０から出力されたライセンス鍵Ｋｃによって復号してコンテンツデータＤｃを取得する（ステップＳ７４４）。

【０１５７】そして、復号されたコンテンツデータＤｃは音楽再生部１５１８へ出力され、音楽再生部１５１８は、コンテンツデータを再生し、ＤＡ変換器１５１９はディジタル信号をアナログ信号に変換して端子１５３０へ出力する。そして、音楽データは端子１５３０から外部出力装置を介してヘッドホーン１３０へ出力されて再生される（ステップＳ７４６）。これによって再生動作が終了する。

【０１５８】上記においては、メモリカード１１０に記録された暗号化コンテンツデータを携帯電話機１００によって再生する場合について説明したが、メモリカード１１２に記録された暗号化コンテンツデータを携帯電話機１０２によって再生する場合、メモリカード１１４に記録された暗号化コンテンツデータを携帯電話機１０４によって再生する場合、およびメモリカード１１６に記録された暗号化コンテンツデータを携帯電話機１０６によって再生する場合についても図１１および図１２に示すフローチャートに従って再生動作が行なわれる。

【０１５９】図１３は、メモリカード１１０のメモリ１４１５におけるライセンス領域１４１５Ｂとデータ領域１４１５Ｃとを示したものである。データ領域１４１５Ｃには、再生リストファイル１６０とコンテンツファイル１６１１～１６１ｎと、ライセンス管理ファイル１６２１～１６２ｎとが記録されている。コンテンツファイル１６１１～１６１ｎは、受信した暗号化コンテンツデータ｛Ｄｃ｝Ｋｃと付加情報Ｄｃ－ｉｎｆとを１つのファイルとして記録する。また、ライセンス管理ファイル１６２１～１６２ｎは、それぞれ、コンテンツファイル１６１１～１６１ｎに対応して記録されている。

【０１６０】メモリカード１１０は、配信サーバ１０から暗号化コンテンツデータおよびライセンスを受信したとき、暗号化コンテンツデータおよびライセンスをメモリ１４１５に記録する。そして、ライセンスは、メモリ１４１５のライセンス領域１４１５Ｂのエントリ番号によって指定された領域に記録され、メモリ１４１５のデータ領域１４１５Ｃに記録された再生リストファイル１６０のライセンス管理ファイルを読出せば、エントリ番号を取得でき、その取得したエントリ番号によって対応するライセンスをライセンス領域１４１５Ｂから読出すことができる。

【０１６１】また、ライセンス管理ファイル１６２２は、点線で示されているが、実際には記録されていないことを示す。コンテンツファイル１６１２は存在しているがライセンスが無く再生できないことを表しているが、これは、たとえば、携帯電話機が他の携帯電話機から暗号化コンテンツデータだけを受信した場合に相当する。

【０１６２】また、コンテンツファイル１６１３は、点線で示されているが、これは、たとえば、携帯電話機が配信サーバ１０から暗号化コンテンツデータおよびライセンスを受信し、その受信した暗号化コンテンツデータだけを他の携帯電話機へ送信した場合に相当し、ライセンスはメモリ１４１５に存在するが暗号化コンテンツデータが存在しないことを意味する。

【０１６３】本発明においては、配信サーバ１０から携帯電話機１００，１０２，１０４，１０６にそれぞれ装着されたメモリカード１１０，１１２，１１４，１１６に配信された暗号化コンテンツデータは、複数の携帯電話機の間でコピー（複製）される。そして、複製元の携帯電話機１００は、暗号化コンテンツデータを複製するとき、複製対象の暗号化コンテンツデータ｛Ｄｃ｝Ｋｃ

とその暗号化コンテンツデータ｛Ｄｃ｝Ｋｃに対応する付加情報Ｄｃ－ｉｎｆとを装着されたメモリカード１１０から読出し、その読出した暗号化コンテンツデータ｛Ｄｃ｝Ｋｃに付加情報Ｄｃ－ｉｎｆと携帯電話機１００の個人情報とを付加した複製データを作成する。そして、携帯電話機１００は、複製データを複製先の携帯電話機１０２へ送信する。

【０１６４】複製先の携帯電話機１０２は、携帯電話機１００から複製データを受信する。そして、携帯電話機１０２においては、複製データから暗号化コンテンツデータ｛Ｄｃ｝Ｋｃ、付加情報Ｄｃ－ｉｎｆ、および複製元の個人情報が取得され、暗号化コンテンツデータ｛Ｄｃ｝Ｋｃは、携帯電話機１０２に装着されたメモリカード１１２に記録される。そして、付加情報Ｄｃ－ｉｎｆおよび複製元の個人情報は複製元に関する情報として携帯電話機１０２のメモリ１１１９に格納される。

【０１６５】携帯電話機１０２のユーザが受信した暗号化コンテンツデータ｛Ｄｃ｝Ｋｃを再生したい場合、図７～図１０に示すフローチャートに従って配信サーバ１０からライセンスを受信する。そして、携帯電話機１０２のユーザは、複製された暗号化コンテンツデータ｛Ｄｃ｝Ｋｃが不必要になったとき、その暗号化コンテンツデータ｛Ｄｃ｝Ｋｃを削除する。その後、携帯電話機１０２のユーザは、複製によって以前に受信した暗号化コンテンツデータ｛Ｄｃ｝Ｋｃが必要になったとき、コンテンツデータの再取得要求を携帯電話機１０２にインプットする。そうすると、携帯電話機１０２は、メモリ１１９に格納された複製元の個人情報に基づいて複製元である携帯電話機１００からコンテンツデータを再取得する。

【０１６６】図１４を参照して、暗号化コンテンツデータの複製時に、複製元である携帯電話機１００において生成される複製データのデータフォーマットについて説明する。複製データ４０は、ヘッダ５０とエレメント５１～５ｎとから成る。ヘッダ５０は、複製対象である暗号化コンテンツデータの付加情報を主に含む。具体的には、ヘッダ５０は、コンテンツＩＤ５０１と、コンテンツ名５０２と、アーチスト名５０３と、サイズ５０４と、日付５０５とを格納する。コンテンツＩＤ５０１は、複製対象である暗号化コンテンツデータを識別するための識別番号である。コンテンツ名５０２は、複製対象である暗号化コンテンツデータの名称である。アーチスト名５０３は、複製対象である暗号化コンテンツデータの著作者名である。サイズ５０４は、複製対象である暗号化コンテンツデータのデータサイズである。日付５０５は、複製を行なう日時である。

【０１６７】複製対象である暗号化コンテンツデータおよび携帯電話機１００のユーザの個人情報は、エレメント５１～５ｎのいずれかに格納される。たとえば、暗号化コンテンツデータは、エレメント５１に格納され、個人情報はエレメント５３に格納される。なお、ヘッダ５０に記載したコンテンツ名５０２、アーチスト名５０３および日付５０５は、エレメント５１～５ｎのいずれか（たとえば、メタエレメント）に格納する構成としてもよい。また、コンテンツ名５０２、アーチスト名５０３および日付５０５は、コンテンツファイル１６１１～１６１ｎに記録されるため、コンテンツファイル１６１１～１６１ｎから取得する構成としてもよい。

【０１６８】複製元である携帯電話機１００は、作成された複製データ４０を複製先である携帯電話機１０２へ送信する。

【０１６９】図１５を参照して、複製先である携帯電話機１０２における複製元に関する情報の管理について説明する。携帯電話機１０２においては、受信した複製データ４０のヘッダ５０からコンテンツＩＤ５０１、コンテンツ名５０２、アーチスト名５０３、サイズ５０４、および日付５０５が取得され、エレメント５１から暗号化コンテンツデータが取得され、エレメント５３から携帯電話機１００のユーザの個人情報が取得される。なお、取得された暗号化コンテンツデータは、携帯電話機１０２に装着されたメモリカード１１２に記録される。

【０１７０】携帯電話機１０２のメモリ１１１９は、図１６に示すデータベース４００を保持している。データベース４００は、コンテンツ番号、コンテンツ名、アーチスト名、サイズ、日付、電話番号、Ｅ－Ｍａｉｌ、カード番号、およびその他の項目から成る。取得されたコンテンツＩＤ５０１、コンテンツ名５０２、アーチスト名５０３、サイズ５０４、および日付５０５は、データベース４００のそれぞれコンテンツ番号、コンテンツ名、アーチスト名、サイズ、および日付の項目に格納され、取得された個人情報は、データベース４００のそれぞれ電話番号、Ｅ－ＭＡｉｌ、カード番号、およびその他の項目に格納される。なお、Ｅ－Ｍａｉｌは、複製元である携帯電話機１００のユーザ所有する電子メールアドレス情報であり、電話番号は、携帯電話機１００の電話番号であり、カード番号は、携帯電話機１００のユーザが所有してクレジットカードの番号である。

【０１７１】このようにして、複製先の携帯電話機１０２においては、複製対象である暗号化コンテンツデータ｛Ｄｃ｝Ｋｃの付加情報Ｄｃ－ｉｎｆと複製元の個人情報とから複製元に関する情報が作成され、メモリ１１１９に格納される。なお、データベース４００は、ｎ個の複製元に関する情報を格納可能である。

【０１７２】そして、携帯電話機１０２のユーザから複製元に関する情報の表示要求がなされると、データベース４００の格納されたｎ個の複製元に関する情報が表示パネル１１１８に表示される。この場合、表示パネル１１１６における１つの複製元に関する情報の表示画面は、図１７に示すとおりである。

【０１７３】図１６を参照して、表示画面６０は、タイ

トル名６１、コンテンツＩＤ６２、アーチスト名６３、サイズ６４、電話番号６５、カード番号６６、Ｅ－ｍａｉｌ６７、コピーした日時６８、その他、６９、再取得ボタン７０、およびキャンセルボタン７１から成る。タイトル名６１には、データベース４００から読出されたコンテンツ名に格納された内容が表示され、コンテンツＩＤ６２には、データベース４００から読出されたコンテンツＩＤが表示され、アーチスト名６３には、データベース４００から読出されたアーチスト名に格納された内容が表示され、サイズ６４には、データベース４００から読出されたサイズに格納された内容が表示され、電話番号６５には、データベース４００から読出された電話番号に格納された内容が表示され、カード番号６６には、データベース４００から読出されたカード番号に格納された内容が表示され、Ｅ－ｍａｉｌ６７には、データベース４００から読出されたＥ－Ｍａｉｌに格納された内容が表示され、コピーした日時６８には、データベース４００から読出された日付に格納された内容が表示され、その他６９には、データベース４００から読出されたその他に格納された内容が表示される。

【０１７４】そして、携帯電話機１０２のユーザは、表示画面６０を見て、コンテンツデータを複製元から再取得するか否かを決定する。ユーザは、コンテンツデータを再取得するとき、再取得ボタン７０を押し、コンテンツデータを再取得しないとき、キャンセルボタン７１を押す。なお、キャンセルボタン７１を押したとき、データベース４００に格納された次の複製元に関する情報が画面６０のフォーマットで表示される。

【０１７５】複製元である携帯電話機１００から複製先である携帯電話機１０２への暗号化コンテンツデータ｛Ｄｃ｝Ｋｃの複製動作について説明する。図１７は、携帯電話機１００から携帯電話機１０２への暗号化コンテンツデータ｛Ｄｃ｝Ｋｃの複製動作を説明するためのフローチャートである。

【０１７６】図１７を参照して、携帯電話機１００のユーザによって操作パネル１１１６から複製リクエストが入力されると（ステップＳ２００）、コントローラ１１２０は、バスＢＳ２を介して複製リクエストを受け、バスＢＳ２およびメモリカードインタフェース１２００を介して暗号化コンテンツデータ｛Ｄｃ｝Ｋｃおよび付加情報Ｄｃ－ｉｎｆの出力要求をメモリカード１１０へ入力する（ステップＳ２０２）。

【０１７７】そうすると、メモリカード１１０においては、コントローラ１４２０は、端子１４２６、インタフェース１４２４、およびバスＢＳ３を介して暗号化コンテンツデータ｛Ｄｃ｝Ｋｃおよび付加情報Ｄｃ－ｉｎｆの出力要求を受理し（ステップＳ２０４）、バスＢＳ３を介してメモリ１４１５から暗号化コンテンツデータ｛Ｄｃ｝Ｋｃおよび付加情報Ｄｃ－ｉｎｆを読出し、その読出した暗号化コンテンツデータ｛Ｄｃ｝Ｋｃおよび付加情報Ｄｃ－ｉｎｆをバスＢＳ３、インタフェース１４２４および端子１４２６を介して携帯電話機１００へ出力する（ステップＳ２０６）。

【０１７８】携帯電話機１００のコントローラ１１２０は、メモリカードインタフェース１２００を介して暗号化コンテンツデータ｛Ｄｃ｝Ｋｃおよび付加情報Ｄｃ－ｉｎｆを受理する（ステップＳ２０８）。そして、コントローラ１１２０は、メモリ１１１９から携帯電話機１００のユーザの個人情報を読出し、暗号化コンテンツデータ｛Ｄｃ｝Ｋｃに付加情報Ｄｃ－ｉｎｆおよび個人情報を付加して複製データを生成する（ステップＳ２１０）。具体的には、コントローラ１１２０は、暗号化コンテンツデータ｛Ｄｃ｝Ｋｃを複製データ４０のエレメント５１に格納し、個人情報をエレメント５３に格納し、付加情報Ｄｃ－ｉｎｆの内容をヘッダ５０のコンテンツＩＤ５０１、コンテンツ名５０２、アーチスト名５０３、およびサイズ５０４に格納し、複製の日時をヘッダ５０の日付５０５に格納して複製データを生成する。そして、コントローラ１１２０は、生成した複製データをバスＢＳ２、送受信部１１０２、およびアンテナ１１００を介して携帯電話機１０２へ送信する（ステップＳ２１２）。

【０１７９】携帯電話機１０２のコントローラ１１２０は、アンテナ１１００、送受信部１１０２、およびバスＢＳ２を介して複製データを受信し（ステップＳ２１４）、その受信した複製データを情報取得部１１２１に与える。情報取得部１１２１は、複製データから暗号化コンテンツデータ｛Ｄｃ｝Ｋｃ、付加情報Ｄｃ－ｉｎｆ、および個人情報を取得し（ステップＳ２１６）、暗号化コンテンツデータ｛Ｄｃ｝ＫｃをバスＢＳ２およびメモリカードインタフェース１２００を介してメモリカード１１２へ入力する（ステップＳ２１８）。

【０１８０】メモリカード１１２においては、コントローラ１４２０は、端子１４２６、インタフェース１４２４およびバスＢＳ３を介して暗号化コンテンツデータ｛Ｄｃ｝Ｋｃを受理し、バスＢＳ３を介してメモリ１４１５のデータ領域１４１５Ｃに暗号化コンテンツデータ｛Ｄｃ｝Ｋｃを記録する（ステップＳ２２０）。

【０１８１】そして、携帯電話機１００のコントローラ１１２０は、付加情報Ｄｃ－ｉｎｆおよび個人情報をメモリ１１１９に格納されたデータベース４００に登録し（ステップＳ２２２）、携帯電話機１００から携帯電話機１０２への暗号化コンテンツデータの複製動作が終了する（ステップＳ２２４）。

【０１８２】このように、暗号化コンテンツデータの複製においては、複製対象である暗号化コンテンツデータに複製元の個人情報を付加して複製先に送信し、複製元の個人情報が複製先において保持される。

【０１８３】なお、携帯電話機１０２のユーザは、携帯電話機１００から受信した暗号化コンテンツデータ｛Ｄ

c｝Ｋｃを復号および再生するためのライセンスを図７～図１０に示すフローチャートに従って配信サーバ１０から受信し、メモリカード１１２に格納する。これによって、携帯電話機１００から複製された暗号化コンテンツデータ｛Ｄｃ｝Ｋｃを復号および再生できる。

【０１８４】携帯電話機１０２のユーザは、携帯電話機１００から複製された暗号化コンテンツデータを復号および再生する。そして、携帯電話機１０２のユーザは、その暗号化コンテンツデータが不用になったとき、メモリカード１１２から暗号化コンテンツデータを削除する。

【０１８５】しかし、携帯電話機１０２のユーザは、その削除した暗号化コンテンツデータが必要になるときがある。次に、携帯電話機１０２のユーザが、削除した暗号化コンテンツデータを携帯電話機１００から再取得する動作について説明する。図１８および図１９は、携帯電話機１０２が携帯電話機１００から暗号化コンテンツデータを再取得する動作を説明するための第１および第２のフローチャートである。

【０１８６】図１８を参照して、携帯電話機１０２のユーザが操作パネル１１１６を介して複製元に関する情報の表示リクエストを入力すると（ステップＳ３００）、携帯電話機１０２のコントローラ１１２０は、バスＢＳ２を介して表示リクエストを受取り、ｎ＝１の設定を行なう（ステップＳ３０２）。そして、コントローラ１１２０は、メモリ１１１９に格納されたデータベース４００のｎ＝１の欄に登録された複製元に関する情報を読出し、その読出した複製元に関する情報をバスＢＳ２を介して表示パネル１１１８に与える。そして、表示パネル１１１８は、複製元に関する情報を画面６０（図１６参照）のフォーマットで表示する（ステップＳ３０４）。

【０１８７】携帯電話機１０２のユーザは、表示パネル１１１６に表示された複製元に関する情報を見て、複製を希望するとき再取得ボタン７０を押し、複製を希望しないときキャンセルボタン７１を押す。携帯電話機１０２のコントローラ１１２０は、再取得ボタン７０が押された否かを判定し（ステップＳ３０６）、キャンセルボタン７１が押されたと判定したとき、ｎ＝ｎ＋１の設定を行ない（ステップＳ３０８）、ステップＳ３０４およびステップＳ３０６を繰返す。つまり、コントローラ１１２０は、ｎ＝２の欄に格納された複製元に関する情報をデータベース４００から読出して表示パネル１１１８に表示し、その表示した画面に基づいて暗号化コンテンツデータの再取得を行なうが否かの判定が行なわれる。

【０１８８】ステップＳ３０６において、コントローラ１１２０は、再取得ボタン７０が押されたと判定したとき、表示画面の電話番号に基づいて携帯電話機１００へ電話を掛け、携帯電話機１００と回線を接続する（ステップＳ３１０）。

【０１８９】そして、携帯電話機１０２のコントローラ１１２０は、表示画面のコンテンツＩＤと、そのコンテンツＩＤによって特定される暗号化コンテンツデータ｛Ｄｃ｝Ｋｃの複製要求とをバスＢＳ２、送受信部１１０２、およびアンテナ１１００を介して携帯電話機１００へ送信する（ステップＳ３１２）。

【０１９０】携帯電話機１００においては、コントローラ１１２０は、アンテナ１１００、送受信部１１０２、およびバスＢＳ２を介してコンテンツＩＤと暗号化コンテンツデータの複製要求とを受信し（ステップＳ３１４）、受信したコンテンツＩＤによって特定される暗号化コンテンツデータの複製が可能か否かを判定する（ステップＳ３１６）。複製不可と判定されたとき、携帯電話機１００のコントローラ１１２０は、複製不可のメッセージを送受信部１１０２およびアンテナ１１００を介して携帯電話機１０２へ送信し、携帯電話機１０２は、複製不可のメッセージをアンテナ１１００、送受信部１１０２、およびバスＢＳ２を介して受信し、複製不可のメッセージを表示パネル１１１８に表示する（ステップＳ３１８）。そして、ステップＳ３０８へ移行し、ステップＳ３０４～Ｓ３１６が繰返される。

【０１９１】ステップＳ３１６において、携帯電話機１００のコントローラ１１２０が複製可と判定したとき図１９に示すステップＳ３２０へ移行する。図１９を参照して、コントローラ１１２０は、コンテンツＩＤと、暗号化コンテンツデータの出力要求とをバスＢＳ２およびメモリカードインタフェース１２００を介してメモリカード１１０へ入力する（ステップＳ３２０）。

【０１９２】そうすると、メモリカード１１０においては、コントローラ１４２０は、端子１４２６、インタフェース１４２４、およびバスＢＳ３を介してコンテンツＩＤと、そのコンテンツＩＤによって特定される暗号化コンテンツデータ｛Ｄｃ｝Ｋｃの出力要求とを受理し（ステップＳ３２２）、バスＢＳ３を介してメモリ１４１５からコンテンツＩＤによって特定される暗号化コンテンツデータ｛Ｄｃ｝Ｋｃを読出し、その読出した暗号化コンテンツデータ｛Ｄｃ｝Ｋｃをバスバス３、インタフェース１４２４および端子１４２６を介して携帯電話機１００へ出力する（ステップＳ３２４）。

【０１９３】携帯電話機１００のコントローラ１１２０は、メモリカードインタフェース１２００を介して暗号化コンテンツデータ｛Ｄｃ｝Ｋｃを受理し、その受理した暗号化コンテンツデータ｛Ｄｃ｝Ｋｃをバスバス２、送受信部１１０２、およびアンテナ１１００を介して携帯電話機１０２へ送信する（ステップＳ３２６）。

【０１９４】携帯電話機１０２のコントローラ１１２０は、アンテナ１１００、送受信部１１０２およびバスＢＳ２を介して暗号化コンテンツデータ｛Ｄｃ｝Ｋｃを受信し、その受信した暗号化コンテンツデータ｛Ｄｃ｝Ｋｃをバスバス２およびメモリカードインタフェース１２００を介してメモリカード１１２へ入力する（ステップ

Ｓ３２８）。

【０１９５】メモリカード１１２においては、コントローラ１４２０は、端子１４２６、インタフェース１４２４およびバスＢＳ３を介して暗号化コンテンツデータ｛Ｄｃ｝Ｋｃを受理し、バスＢＳ３を介してメモリ１４１５のデータ領域１４１５Ｃに暗号化コンテンツデータ｛Ｄｃ｝Ｋｃを記録する（ステップＳ３３０）。

【０１９６】その後、携帯電話機１０２のコントローラ１１２０は、暗号化コンテンツデータの複製が終了したか否かを判定し（ステップＳ３３２）、複製が終了していないとき図１８に示すステップＳ３０４から図１９に示すステップＳ３３２が繰返される。

【０１９７】ステップＳ３３２において、暗号化コンテンツデータの複製が終了したと判定されたとき、コントローラ１１２０は、その旨を表示パネル１１１８に表示し（ステップＳ３３４）、一連の動作が終了する（ステップＳ３３６）。

【０１９８】このように、携帯電話機１０２は、以前に複製した暗号化コンテンツデータの複製元の個人情報を保持することによって、暗号化コンテンツデータを携帯電話機１００から容易に再取得することができる。

【０１９９】上記においては、暗号化コンテンツデータの複製に際して複製元である携帯電話機１００が個人情報を複製対象である暗号化コンテンツデータに付加するとして説明したが（図１７のステップＳ２１０参照）、本発明においては、複製元の個人情報は、複製先である携帯電話機１０２が作成してもよい。その場合、携帯電話機１００から携帯電話機１０２への暗号化コンテンツデータの複製動作は、図２０に示すフローチャートに従って行なわれる。図２０に示すフローチャートは、図１７に示すフローチャートのステップＳ２１０をステップＳ２１０ａに代え、ステップＳ２１６をステップＳ２１６ａに代え、その代えたステップＳ２１６ａとステップＳ２１８との間にステップＳ２１７を挿入したものであり、その他は図１７に示すフローチャートと同じである。

【０２００】図２０を参照して、上述したようにステップＳ２００～Ｓ２０８が実行されると、携帯電話機１００のコントローラ１１２０は、メモリカード１１０から受理した暗号化コンテンツデータ｛Ｄｃ｝Ｋｃに付加情報Ｄｃ－ｉｎｆを付加して複製データを生成する（ステップＳ２１０ａ）。具体的には、コントローラ１１２０は、暗号化コンテンツデータ｛Ｄｃ｝Ｋｃを複製データ４０のエレメント５１に格納し、付加情報Ｄｃ－ｉｎｆの内容をヘッダ５０のコンテンツＩＤ５０１、コンテンツ名５０２、アーチスト名５０３、およびサイズ５０４に格納し、複製の日時をヘッダ５０の日付５０５に格納する。

【０２０１】その後、上述したようにステップＳ２１２，Ｓ２１４が実行されると、携帯電話機１０２のコントローラ１１２０は、複製データを情報取得部１１２１に与え、情報取得部１１２１は、複製データから暗号化コンテンツデータ｛Ｄｃ｝Ｋｃおよび付加情報Ｄｃ－ｉｎｆを取得する（ステップＳ２１６ａ）。そして、コントローラ１１２０は、複製元の電話番号（複製データの受信時に携帯電話機１００から受信する）から携帯電話機１００の個人情報を生成する（ステップＳ２１７）。その後、ステップＳ２１８～Ｓ２２４が上述したように実行され、暗号化コンテンツデータの複製動作が終了する。

【０２０２】このように、複製元が個人情報を暗号化コンテンツデータに付加しないとき、複製先が複製元の個人情報を作成して保持する。

【０２０３】図２０に示すフローチャートに従って複製された暗号化コンテンツデータを複製元から再取得するとき、複製元に関する情報は、図１６においてカード番号６６およびＥ－ｍａｉｌ６７の部分が空白のまま表示される。これは、複製元である携帯電話機１００から、携帯電話機１００のユーザが所有するホームページのアドレスおよびカード番号が携帯電話機１０２へ送信されないからである。

【０２０４】暗号化コンテンツデータの複製および複製された暗号化コンテンツデータの再取得における複製先の携帯電話機１０２の機能ブロックを示すと図２１に示すようになる。携帯電話機１０２は、コピー元情報取得部８１と、コピー元情報管理部８２と、コピー元情報表示部８３と、コンテンツ再取得処理部８４とを含む。

【０２０５】コピー元情報取得部８１は、複製元である携帯電話機１００から受信した複製データから暗号化コンテンツデータ｛Ｄｃ｝Ｋｃ、付加情報Ｄｃ－ｉｎｆ、および個人情報を取得し、その取得した付加情報Ｄｃ－ｉｎｆおよび個人情報をコピー元情報管理部に格納されたデータベース４００に登録する。

【０２０６】コピー元情報管理部８２は、図１５に示すデータベース４００を格納する。コピー元情報表示部８３は、コピー元情報管理部８２に格納されたデータベース４００から複製元に関する情報を読出し、その読出した複製元に関する情報を表示する。コンテンツ再取得処理部８４は、複製された暗号化コンテンツデータを複製元から再取得する処理を行なう。

【０２０７】したがって、図５に示す携帯電話機１０２の構成のうち、コントローラ１１２０および情報取得部１１２１は、コピー元情報取得部８１を構成し、メモリ１１１９は、コピー元情報管理部８２を構成し、表示パネル１１１８およびコントローラ１１２０はコピー元情報表示部８３およびコンテンツ再取得処理部８４を構成する。

【０２０８】上記においては、複製対象のコンテンツデータを公開鍵暗号方式によって配信サーバ１０から携帯電話機１００，１０２，１０４，１０６に配信された暗

号化コンテンツデータであるとして説明したが、本発明においては、複製対象のコンテンツデータは、インターネットを介して取得される暗号化されていないコンテンツデータであってもよい。すなわち、インターネットを介して携帯電話機へ配信されたコンテンツデータ、インターネットを介してパーソナルコンピュータへ配信されたコンテンツデータをケーブルを介して携帯電話機へ送信されたコンテンツデータ、およびパーソナルコンピュータがＣＤリッピングによって取得したコンテンツデータをケーブルを介して携帯電話機へ送信されたコンテンツデータ等が複製対象となる。つまり、コンテンツデータの取得経路は問わない。これらのコンテンツデータの複製および再取得の動作についても、図１７～図２０に示すフローチャートに従って行なわれる。

【０２０９】本発明の実施の形態によれば、コンテンツデータを複製するとき、複製先の携帯電話機は、複製元の個人情報を複製元の携帯電話機から受信して保持するので、その複製されたコンテンツデータを削除しても複製元の携帯電話機からその削除したコンテンツデータを容易に再取得できる。

【０２１０】今回開示された実施の形態はすべての点で例示であって制限的なものではないと考えられるべきである。本発明の範囲は、上記した実施の形態の説明ではなくて特許請求の範囲によって示され、特許請求の範囲と均等の意味および範囲内でのすべての変更が含まれることが意図される。

【図面の簡単な説明】

【図１】　データ配信システムを概念的に説明する概略図である。

【図２】　図１に示すデータ配信システムにおける通信のためのデータ、情報等の特性を示す図である。

【図３】　図１に示すデータ配信システムにおける通信のためのデータ、情報等の特性を示す図である。

【図４】　図１に示すデータ配信システムにおける配信サーバの構成を示す概略ブロック図である。

【図５】　図１に示すデータ配信システムにおける携帯電話機の構成を示す概略ブロック図である。

【図６】　図１に示すデータ配信システムにおけるメモリカードの構成を示す概略ブロック図である。

【図７】　図１に示すデータ配信システムにおけるコンテンツデータの配信動作を説明するための第１のフローチャートである。

【図８】　図１に示すデータ配信システムにおけるコンテンツデータの配信動作を説明するための第２のフローチャートである。

【図９】　図１に示すデータ配信システムにおけるコンテンツデータの配信動作を説明するための第３のフローチャートである。

【図１０】　図１に示すデータ配信システムにおけるコンテンツデータの配信動作を説明するための第４のフローチャートである。

【図１１】　携帯電話機における再生動作を説明するための第１のフローチャートである。

【図１２】　携帯電話機における再生動作を説明するための第２のフローチャートである。

【図１３】　メモリカードにおける再生リストファイルの構成を示す図である。

【図１４】　複製データのフォーマットである。

【図１５】　複製元に関する情報を登録するデータベースを示す図である。

【図１６】　コンテンツデータの再取得時に携帯電話機の表示パネルに表示される画面を示す図である。

【図１７】　暗号化コンテンツデータの複製動作を説明するためのフローチャートである。

【図１８】　複製された暗号化コンテンツデータを再取得する動作を説明するための第１のフローチャートである。

【図１９】　複製された暗号化コンテンツデータを再取得する動作を説明するための第２のフローチャートである。

【図２０】　暗号化コンテンツデータの複製動作を説明するための他のフローチャートである。

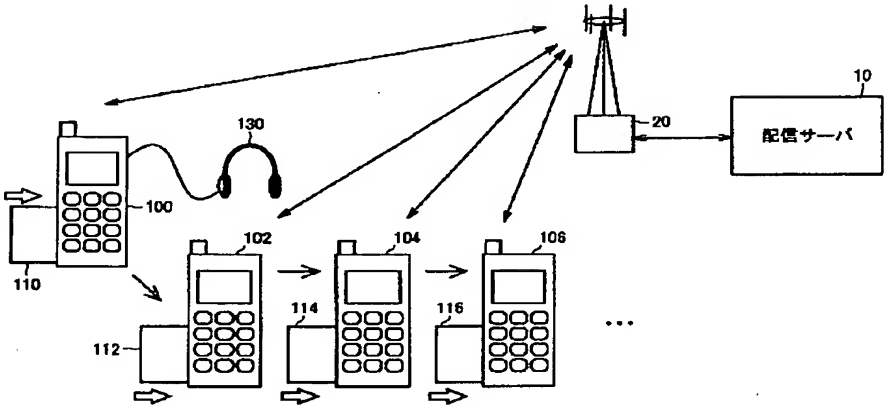
【図２１】　コンテンツデータの複製動作および再取得動作を行なう携帯電話機の機能ブロックを示す図である。

【符号の説明】

１０　配信サーバ、２０　配信キャリア、４０　複製データ、５０　ヘッダ、５１～５ｎ　エレメント、６０　画面、６１　タイトル名、６２，５０１　コンテンツＩＤ、６３，５０３　アーチスト名、６４，５０４　サイズ、６５　電話番号、６６　カード番号、６７　Ｅ－ｍａｉｌ、６８　コピー日時、６９　その他、７０　再取得ボタン、７１　キャンセルボタン、８１　コピー元情報取得部、８２　コピー元情報管理部、８３　コピー元情報表示部、８４　コンテンツ再取得処理部、１００，１０２，１０４，１０６　携帯電話機、１１０，１１２，１１４，１１６　メモリカード、１３０　ヘッドホーン、１６０　再生リストファイル、３５０　通信装置、３０２　課金データベース、３０４　情報データベース、３０６　ＣＲＬデータベース、３０７　メニューデータベース、３０８配信記録データベース、３１０　データ処理部、３１２，３２０，１４０４，１４０８，１４１２，１４２２，１５０４，１５１０，１５１６　復号処理部、３１３　認証鍵保持部、３１５　配信制御部、３１６　セッションキー発生部、３１８，３２６，３２８，１４０６，１４１０，１４１７，１５０６　暗号処理部、４００　データベース、５０２　コンテンツ名、５０５　日付、１１２０，１４２０　コントローラ、１４２６，１５３０　端子、１１００　アンテナ、１１０２　送受信部、１１０４　マイク、１１０６　Ａ

Ｄ変換器、１１０８　音声符号化部、１１１０　音声再生部、１１１２　ＤＡ変換器、１１１４　スピーカ、１１１６　操作パネル、１１１８　表示パネル、１１１９，１４１５　メモリ、１１２１　情報取得部、１２００　メモリカードインタフェース、１４００，１５００　認証データ保持部、１４０２　Ｋｍｃ保持部、１４１４　ＫＰａ保持部、１４１５Ａ　ＣＲＬ領域、１４１５Ｂ　ライセンス領域、１４１５Ｃ　データ領域、１４１＊６　ＫＰｍｃ保持部、１４１８　セッションキー発生部、１４２１Ｋｍ保持部、１４２４　インタフェース、１４４２，１４４６　切換スイッチ、１５０２　Ｋｐ１保持部、１５１８　音楽再生部、１５１９　ＤＡ変換器、１６２１～１６２ｎ　ライセンス管理ファイル、１６１１～１６１ｎ　コンテンツファイル、１５５０　コンテンツ再生デバイス。

【図１】



【図２】

記号	種類	属性	特性
Dc	コンテンツデータ	コンテンツ固有	例：音楽データ、朗読データ、教材データ、画像データ Kcにて復号可能な暗号化コンテンツデータ {Dc}Kcとして配信され、メモリカードに保持される
Dc-inf	付加情報	コンテンツ固有	Dcに付随する平文データ。
Kc	ライセンス	コンテンツ固有	ライセンス 暗号化コンテンツデータを復号する復号鍵
ACm/ACp	ライセンス	ライセンス固有	制限情報 再生やライセンスの取り扱いに対する制限事項
トランザクションID	ライセンス	ライセンス固有	配信を特定するための管理コード
コンテンツID	ライセンス	コンテンツ固有	コンテンツを特定するための管理コード
ライセンスID	ライセンス	ライセンス固有	トランザクションID＋コンテンツIDの総称
ライセンス	ライセンス	ライセンス固有	Kc＋ACm＋ACp＋ライセンスIDの総称
CRL	禁止クラスリスト	システム共通	使用禁止認証データのリスト CRLの更新日(CRLdate)を含む

【図１５】

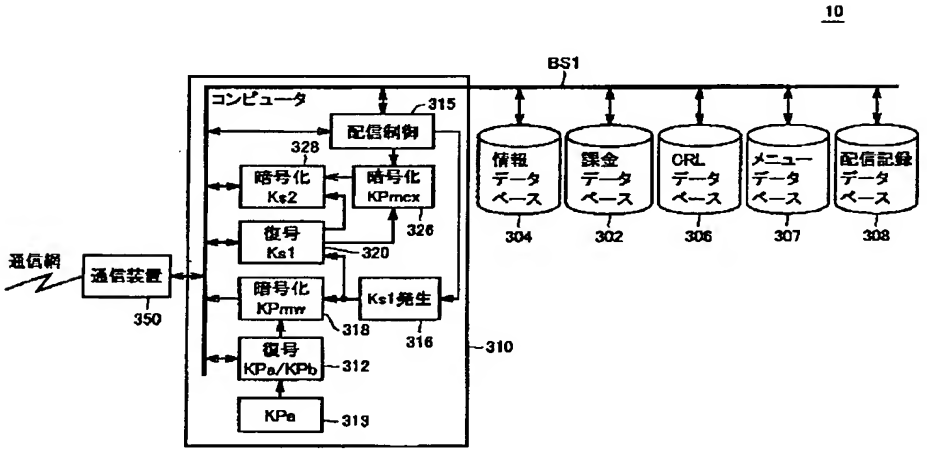
400

	コンテンツ番号	コンテンツ名	アーチスト名	サイズ	日　付	電話番号	E-Mail	カード番号	その他
1									
2									
	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮
n									

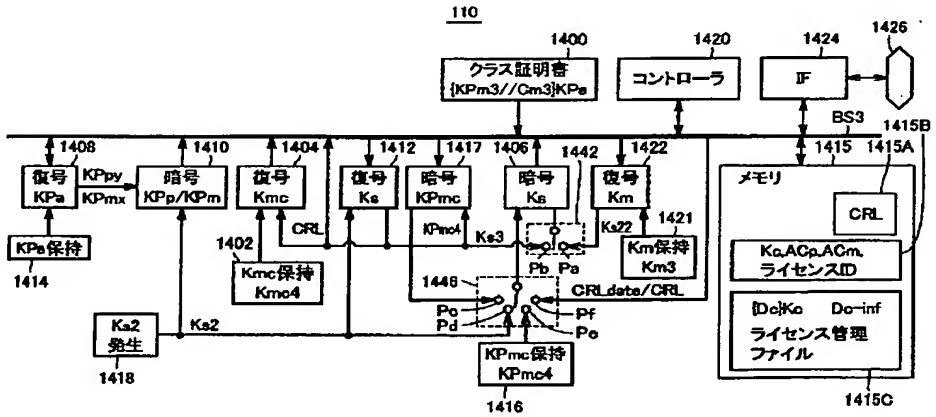
【図３】

	記号	意味	属性	特性
配信サーバ	KPa	公開認証鍵	システム共通	認証局にて認証データを復号する鍵
	Ks1	共通鍵	セッション固有	メモリカードへのライセンスの配信ごとに発生
メモリカード	KPa	公開認証鍵	システム共通	認証局にて認証データを復号する鍵 配信サーバのKPaと同一
	KPmw	公開暗号鍵	クラス固有	証明書Cmwとともに認証局にて暗号化された認証データとして保持 wはクラスを識別するための識別子
	Kmw	秘密復号鍵	クラス固有	公開暗号鍵KPmwにて暗号化されたデータを復号する非対称な復号鍵
	KPmcx	公開暗号鍵	個別	メモリカードごとに異なる。 xはモジュールを識別するための識別子
	Kmcx	秘密復号鍵	個別	公開暗号鍵KPmcxにて暗号化されたデータを復号する非対称な復号鍵
	Ks2	共通鍵	セッション固有	配信サーバまたは音楽再生モジュール間のライセンスの授受ごとに発生
	Cmw	証明書	クラス証明書	メモリカードのクラス証明書。認証機能を有する。 {KPmw//Cmw}KPa又は{KPmw//Cmw}KPbの形式で出荷時に記録。 ＊メモリカードのクラスwごとに異なる。
コンテンツ再生デバイス	KPpy	公開暗号鍵	クラス固有	証明書Cmwとともに認証局にて暗号化された認証データとして保持 yはクラスを識別するための識別子
	Kpy	秘密復号鍵	クラス固有	公開暗号鍵KPpyにて暗号化されたデータを復号する非対称な復号鍵
	Ks3	共通鍵	セッション固有	配信サーバまたは音楽再生モジュール間の再生セッションごとに発生
	Cpy	証明書	クラス証明書	コンテンツ再生デバイスのクラス証明書。認証機能を有する。 {KPpy//Cpy}KPaの形式で出荷時に記録。 ＊コンテンツ再生デバイスのクラスyごとに異なる。

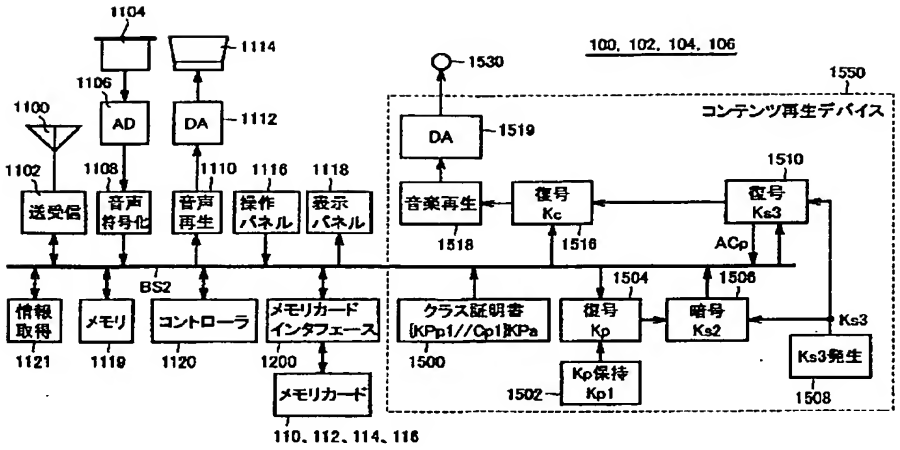
【図４】



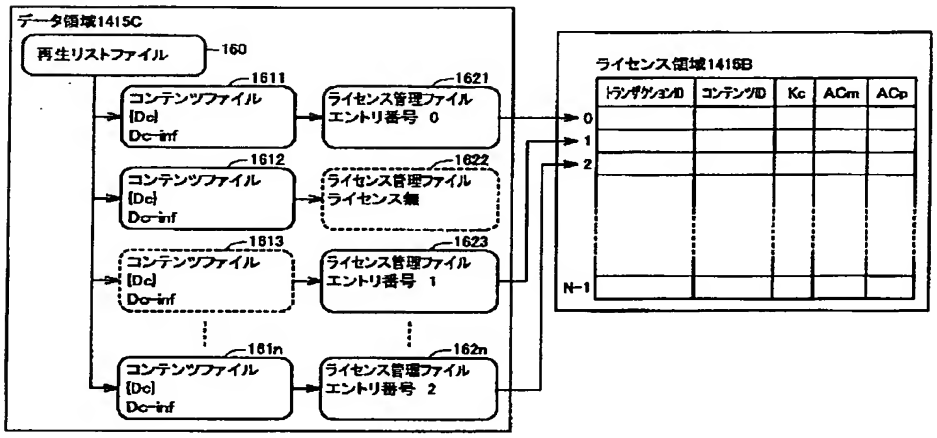
【図６】



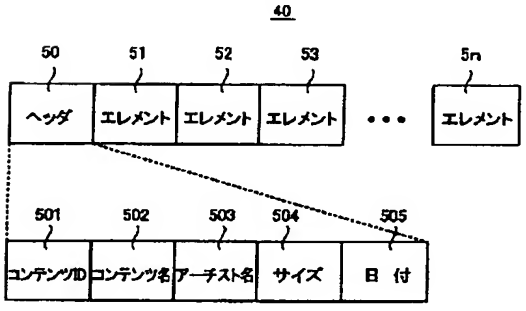
【図５】



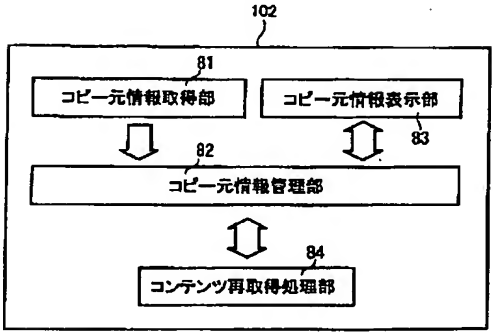
【図１３】



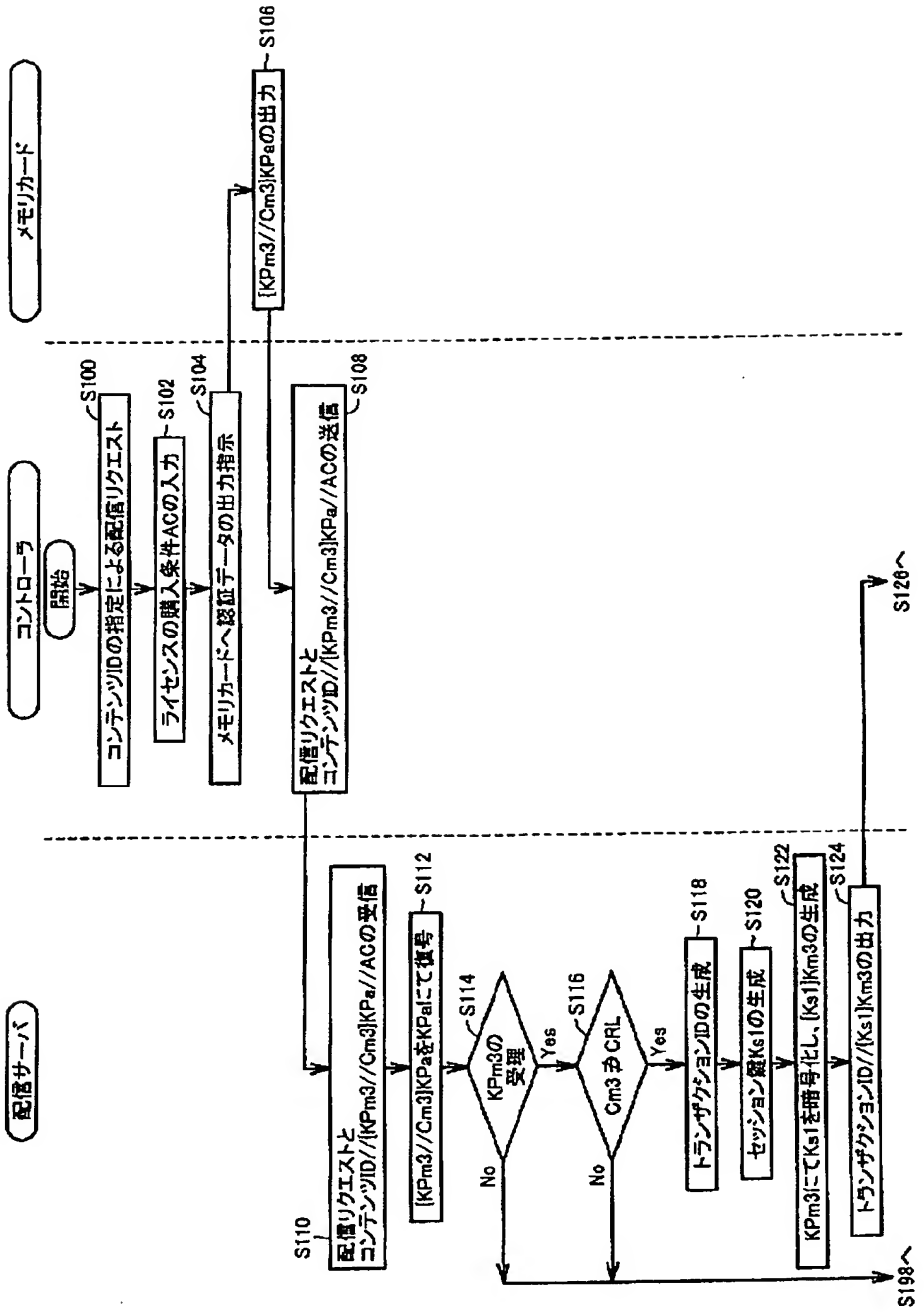
【図１４】



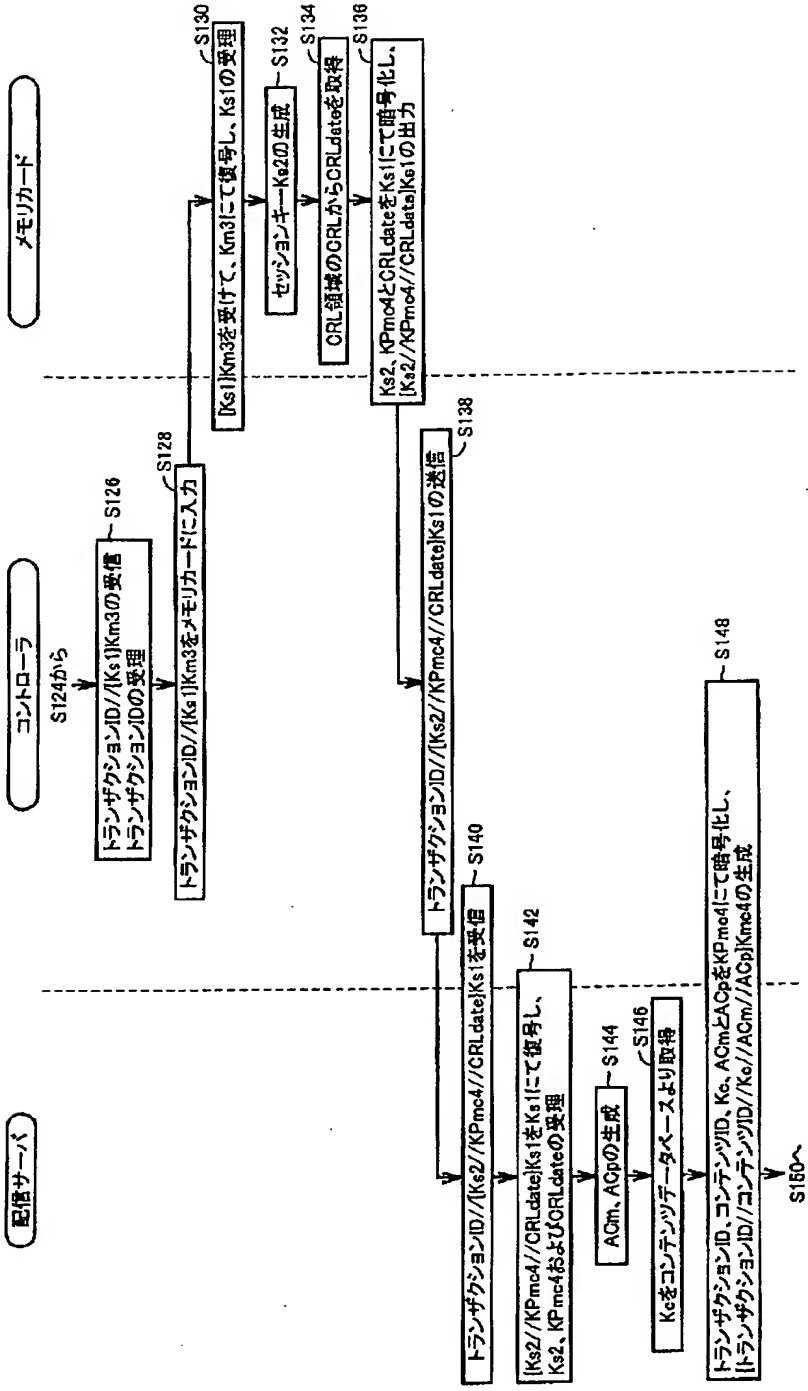
【図２１】



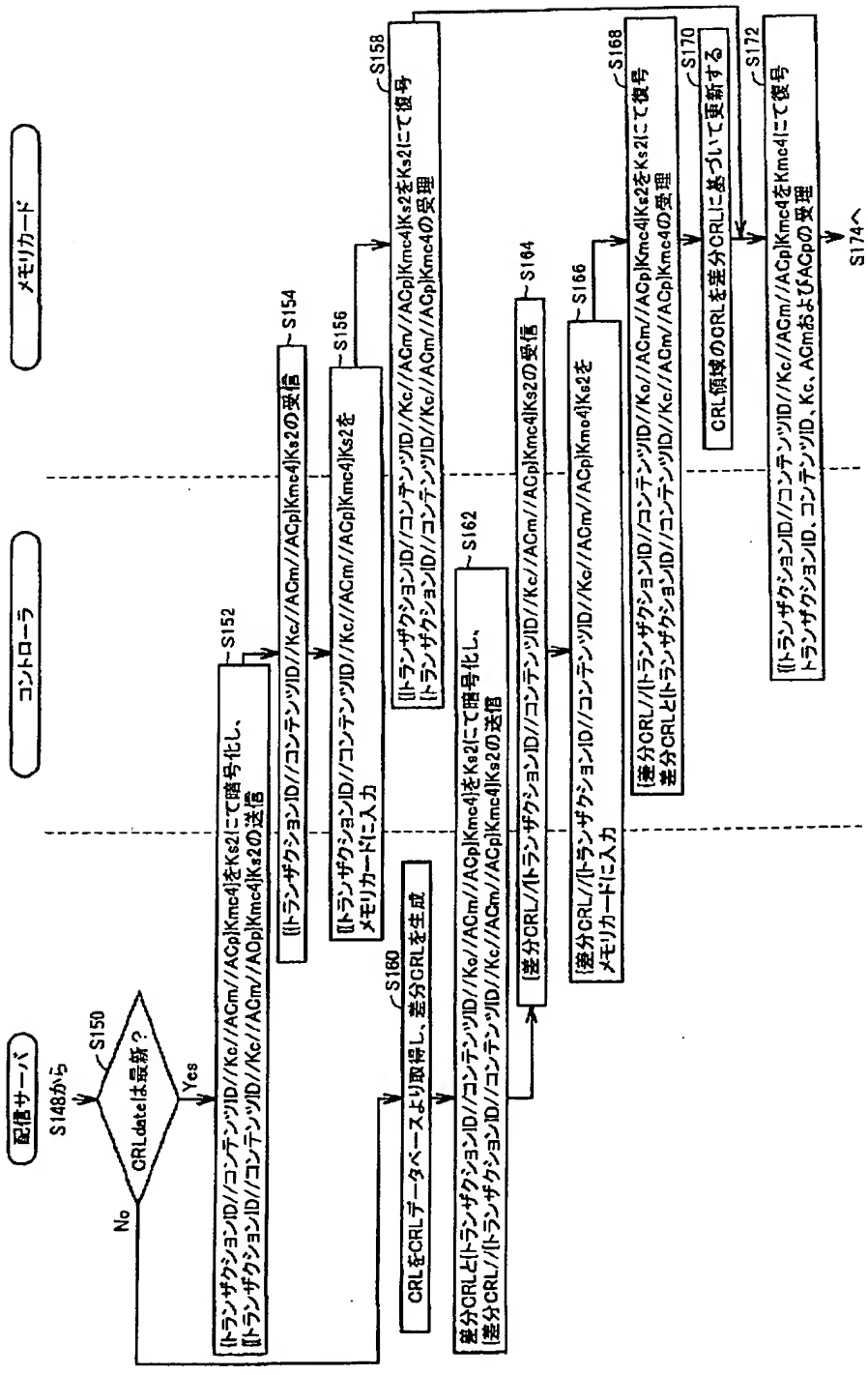
【図７】


メモリカード
コントローラ
配信サーバ
開始
S100
コンテンツIDの指定による配信リクエスト
S102
ライセンスの購入条件ACの入力
S104
メモリカードへ認証データの出力指示
S106
[KPm3//Cm3]KPaの出力
S108
配信リクエストと
コンテンツID//[KPm3//Cm3]KPa//ACの送信
S110
配信リクエストと
コンテンツID//[KPm3//Cm3]KPa//ACの受信
S112
[KPm3//Cm3]KPaをKPaにて復号
S114
KPm3の
受理
No
Yes
S116
Cm3 ≠ CRL
No
Yes
S118
トランザクションIDの生成
S120
セッション鍵Ks1の生成
S122
KPm3にてKs1を暗号化し、[Ks1]Km3の生成
S124
トランザクションID//[Ks1]Km3の出力
S120へ
S198へ

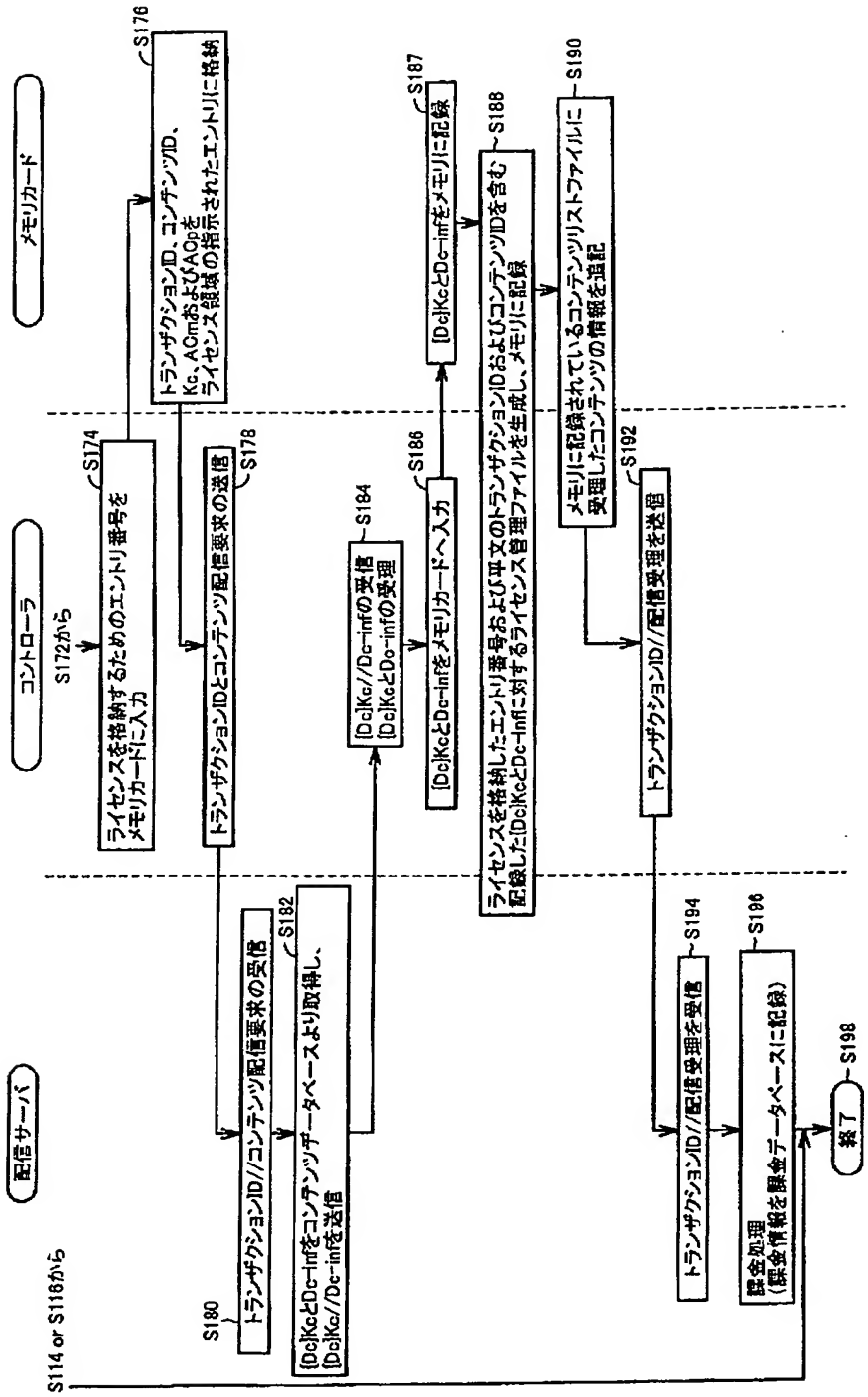
【図８】


メモリカード
コントローラ
配信サーバ
S124から
S126
トランザクションID//{Ks1}Km3の受信
トランザクションIDの受理
S128
トランザクションID//{Ks1}Km3をメモリカードに入力
S130
{Ks1}Km3を受けて、Km3にて復号し、Ks1の受理
S132
セッションキーKs2の生成
S134
CRL領域のCRLからCRLdateを取得
S136
Ks2、KPmc4とCRLdateをKs1にて暗号化し、
{Ks2//KPmc4//CRLdate}Ks1の出力
S138
トランザクションID//{Ks2//KPmc4//CRLdate}Ks1の送信
S140
トランザクションID//{Ks2//KPmc4//CRLdate}Ks1を受信
S142
{Ks2//KPmc4//CRLdate}Ks1を1にて復号し、
Ks2、KPmc4およびCRLdateの受理
S144
ACm、ACpの生成
S146
Kcをコンテンツデータベースより取得
S148
トランザクションID、コンテンツID、Kc、ACmとACpをKPmc4にて暗号化し、
{トランザクションID//コンテンツID//Kc//ACm//ACp}Kmc4の生成
S150へ

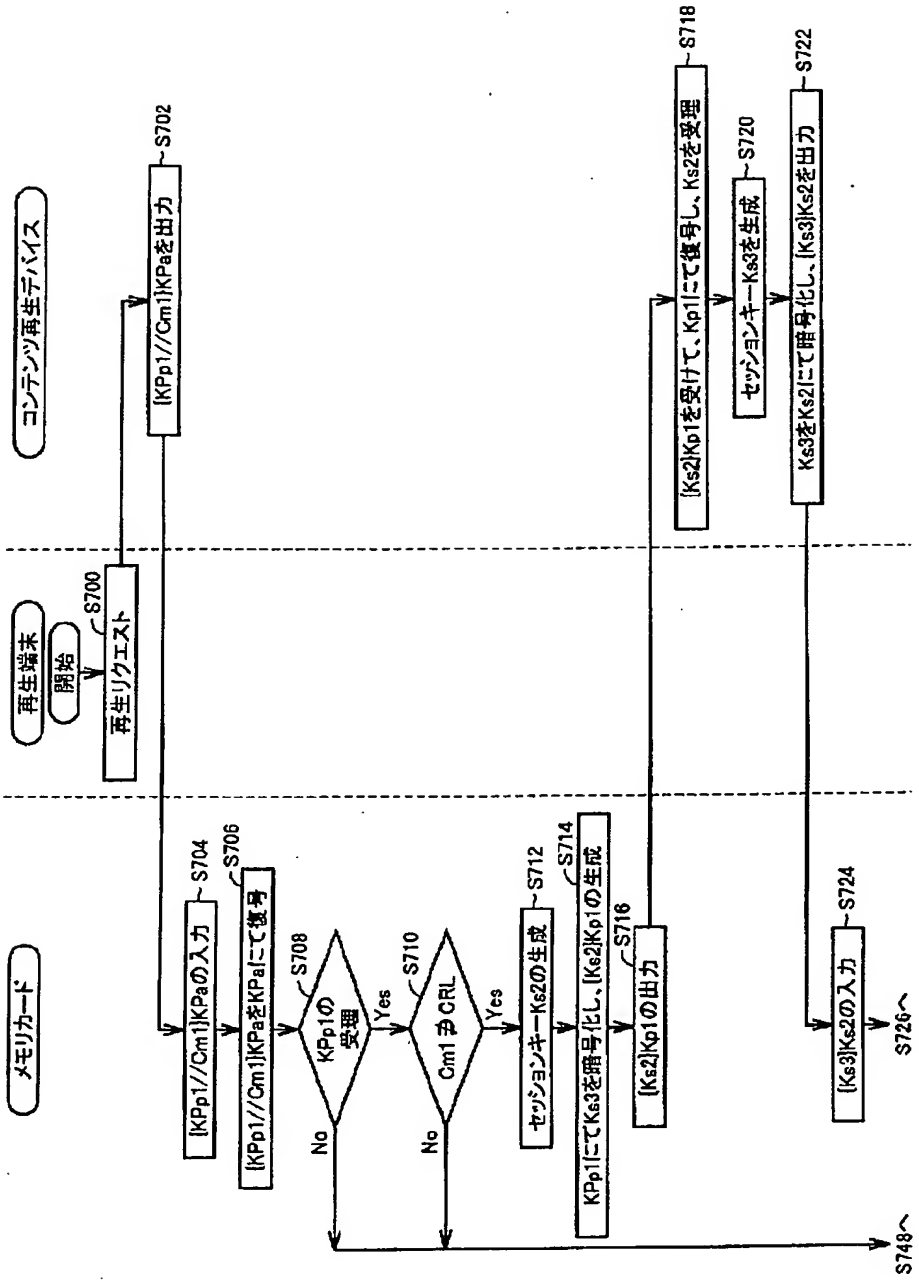
【図9】


配信サーバ
コントローラ
メモリカード
S148から
S150
CRL dateは最新？
No
Yes
S152
S154
S156
S158
S160
S162
S164
S166
S168
S170
S172
S174へ
[[トランザクションID//Kc//ACm//ACp]Kmc4]Ks2にて暗号化し、
[[トランザクションID//Kc//ACm//ACp]Kmc4]Ks2の送信
[[トランザクションID//Kc//ACm//ACp]Kmc4]Ks2の受信
[[トランザクションID//Kc//ACm//ACp]Kmc4]Ks2を
メモリカードに入力
[[トランザクションID//Kc//ACm//ACp]Kmc4]Ks2をKs2にて復号
[[トランザクションID//コンテンツID//Kc//ACm//ACp]Kmc4]Ks2をKs2にて復号
[[トランザクションID//Kc//ACm//ACp]Kmc4]Ks2の受理
CRL領域のCRLを差分CRLに基づいて更新する
[[トランザクションID//コンテンツID//Kc//ACm//ACp]Kmc4]をKmc4にて復号
トランザクションID、コンテンツID、Kc、ACmおよびACpの受理
CRLをCRLデータベースより取得し、差分CRLを生成
差分CRLと[[トランザクションID//Kc//ACm//ACp]Kmc4]をKs2にて暗号化し、
[差分CRL//[トランザクションID//Kc//ACm//ACp]Kmc4]Ks2の送信
[差分CRL//[トランザクションID//コンテンツID//Kc//ACm//ACp]Kmc4]Ks2の受信
[差分CRL//[トランザクションID//コンテンツID//Kc//ACm//ACp]Kmc4]Ks2を
メモリカードに入力
[差分CRL//[トランザクションID//コンテンツID//Kc//ACm//ACp]Kmc4]Ks2をKs2にて復号
差分CRLと[トランザクションID//コンテンツID//Kc//ACm//ACp]Kmc4の受理

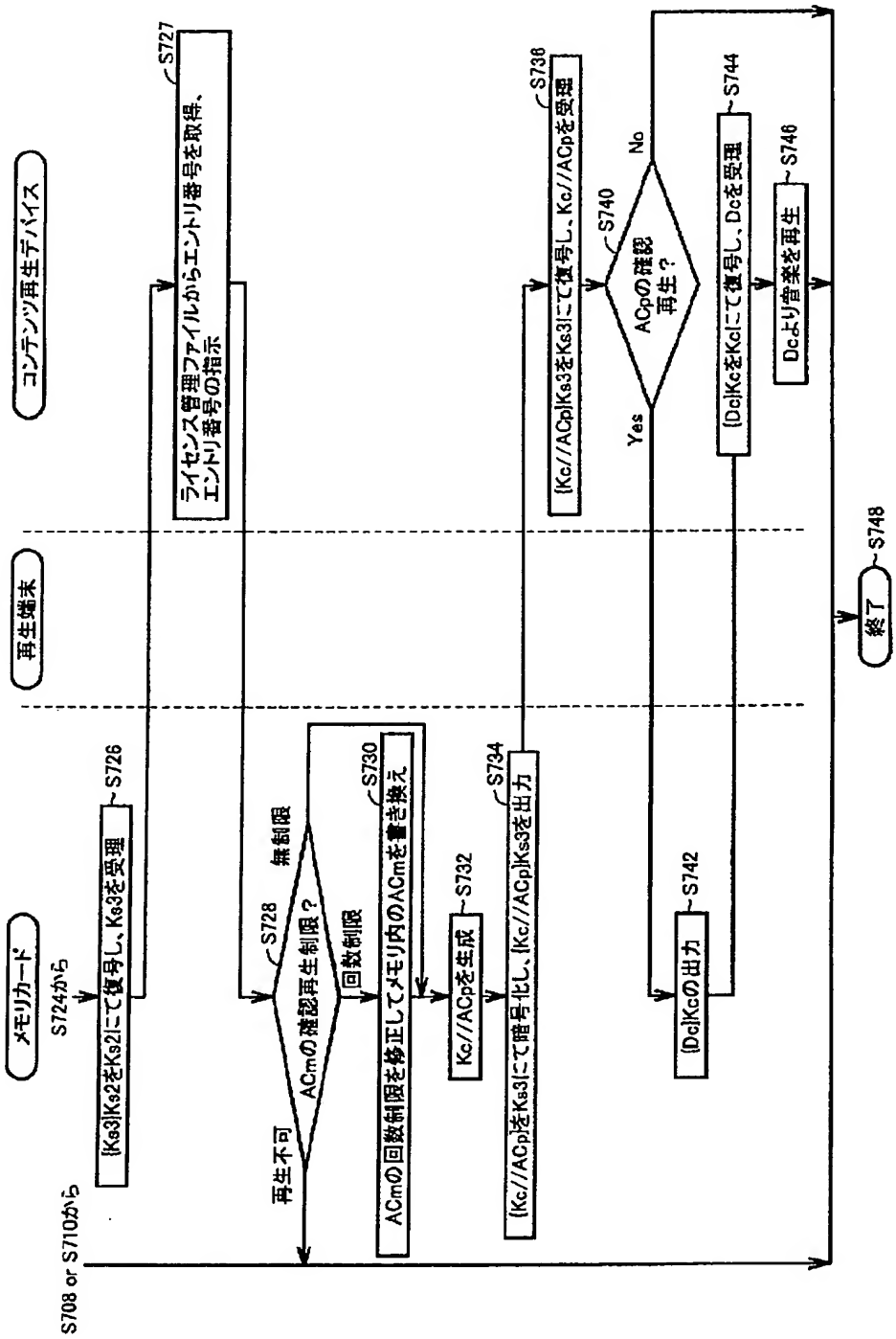
【図１０】


メモリカード
コントローラ
配信サーバ
S172から
S114 or S116から
S174
ライセンスを格納するためのエントリ番号をメモリカードに入力
S176
トランザクションID、コンテンツID、Kc、ACmおよびAOpをライセンス領域の指示されたエントリに格納
S178
トランザクションIDとコンテンツ配信要求の送信
S180
トランザクションID//コンテンツ配信要求の受信
S182
{Dc|Kc}と{Dc-inf}をコンテンツデータベースより取得し、{Dc|Kc}//{Dc-inf}を送信
S184
{Dc|Kc}//{Dc-inf}の受信
{Dc|Kc}と{Dc-inf}の受理
S186
{Dc|Kc}と{Dc-inf}をメモリカードへ入力
S187
{Dc|Kc}と{Dc-inf}をメモリに記録
S188
ライセンスを格納したエントリ番号および平文のトランザクションIDおよびコンテンツIDを含む
記録した{Dc|Kc}と{Dc-inf}に対するライセンス管理ファイルを生成し、メモリに記録
S190
メモリに記録されているコンテンツリストファイルに
受理したコンテンツの情報を追記
S192
トランザクションID//配信受理を送信
S194
トランザクションID//配信受理を受信
S196
課金処理
（課金情報を課金データベースに記録）
S198
終了

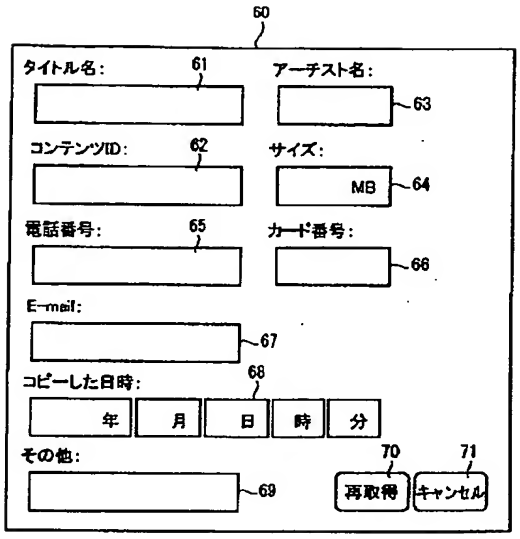
【図１１】


コンテンツ再生デバイス
再生端末
メモリカード
開始
S700
再生リクエスト
S702
[KPp1//Cm1]KPaを出力
S704
[KPp1//Cm1]KPaの入力
S706
[KPp1//Cm1]KPaをKPaにて復号
S708
KPp1の受理
Yes
No
S710
Cm1 予CRL
Yes
No
S712
セッションキーKs2の生成
S714
KPp1にてKs3を暗号化し、[Ks2]Kp1の生成
S716
[Ks2]Kp1の出力
S718
[Ks2]Kp1を受けて、Kp1にて復号し、Ks2を受理
S720
セッションキーKs3を生成
S722
Ks3をKs2にて暗号化し、[Ks3]Ks2を出力
S724
[Ks3]Ks2の入力
S726へ
S748へ

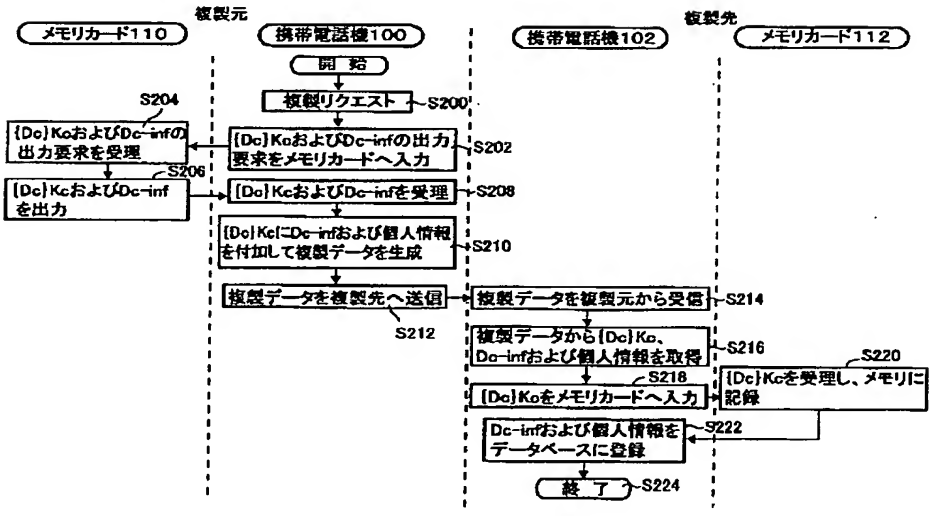
【図１２】


メモリカード
コンテンツ再生デバイス
再生端末
S708 or S710から
S724から
[Ks3]Ks2をKs2にて復号し、Ks3を受理
S726
ライセンス管理ファイルからエントリ番号を取得、
エントリ番号の指示
S727
S728
ACmの確認再生制限？
無制限
回数制限
再生不可
S730
ACmの回数制限を修正してメモリ内のACmを書き換え
Kc//ACpを生成
S732
[Kc//ACp]をKs3にて暗号化し、[Kc//ACp]Ks3を出力
S734
[Kc//ACp]Ks3をKs3にて復号し、Kc//ACpを受理
S736
ACpの確認
再生？
S740
No
Yes
[Dc]Kcの出力
S742
[Dc]KcをKcにて復号し、Dcを受理
S744
Dcより音楽を再生
S746
終了
S748

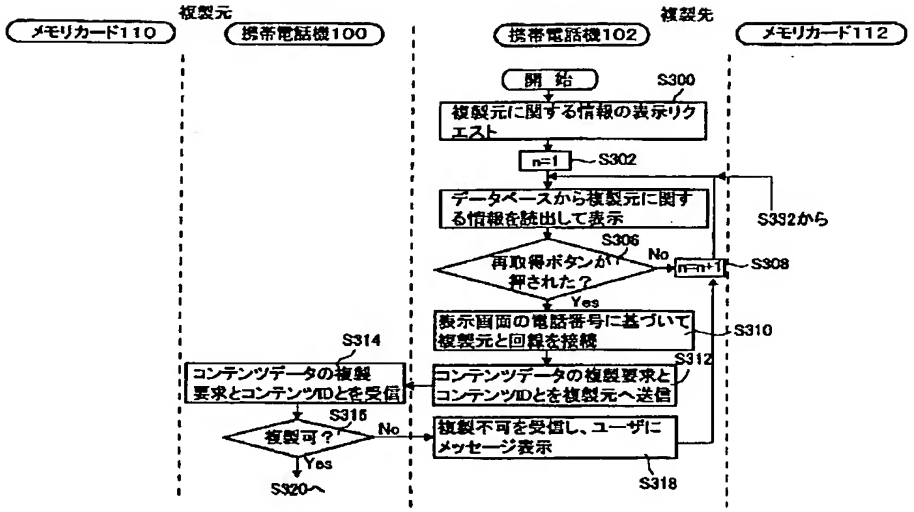
【図１６】


60
タイトル名：
61
アーチスト名：
63
コンテンツID：
62
サイズ：
MB
64
電話番号：
65
カード番号：
66
E-mail：
67
コピーした日時：
68
年
月
日
時
分
その他：
69
70
再取得
71
キャンセル

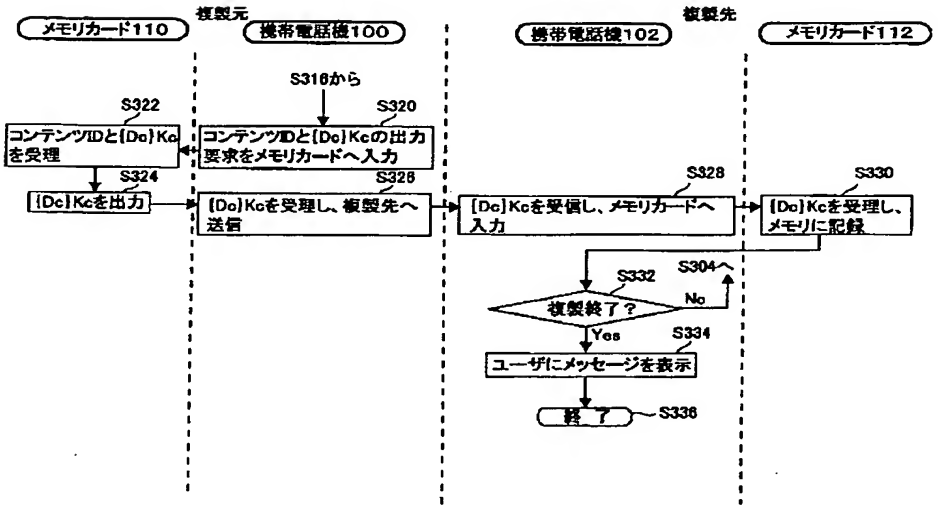
【図１７】


複製元
メモリカード110
携帯電話機100
携帯電話機102
複製先
メモリカード112
開始
複製リクエスト
S200
S204
{Dc}KoおよびDc-infの出力要求を受理
{Dc}KoおよびDc-infの出力要求をメモリカードへ入力
S202
S206
{Dc}KcおよびDc-infを出力
{Dc}KcおよびDc-infを受理
S208
{Dc}KcにDc-infおよび個人情報を付加して複製データを生成
S210
複製データを複製先へ送信
S212
複製データを複製元から受信
S214
複製データから{Dc}Ko、Dc-infおよび個人情報を取得
S216
S220
{Dc}Kcを受理し、メモリに記録
S218
{Dc}Koをメモリカードへ入力
Dc-infおよび個人情報をデータベースに登録
S222
終了
S224

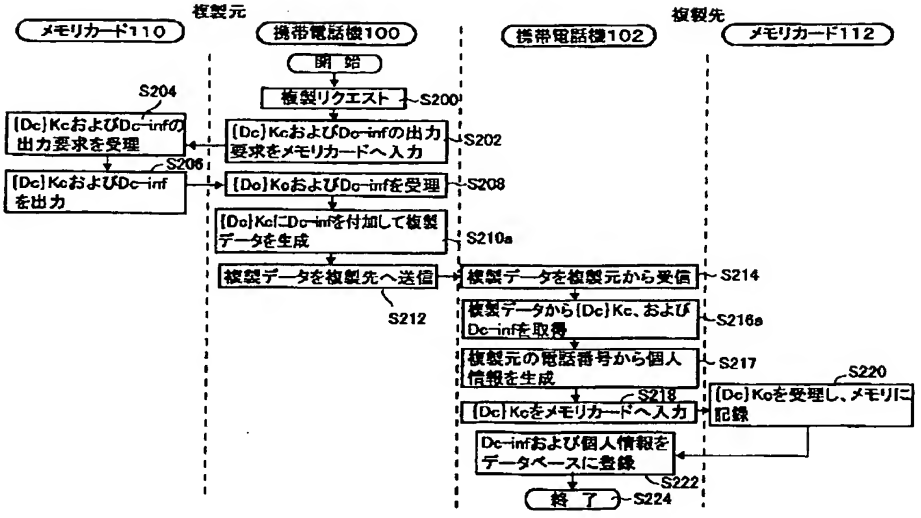
【図１８】


複製元
複製先
メモリカード110
携帯電話機100
携帯電話機102
メモリカード112
開始
S300
複製元に関する情報の表示リクエスト
n=1
S302
データベースから複製元に関する情報を読出して表示
S306
再取得ボタンが押された？
No
n=n+1
S308
S302から
Yes
表示画面の電話番号に基づいて複製元と回線を接続
S310
S312
コンテンツデータの複製要求とコンテンツIDとを複製元へ送信
S314
コンテンツデータの複製要求とコンテンツIDとを受信
S316
複製可？
No
複製不可を受信し、ユーザにメッセージ表示
S318
Yes
S320へ

【図１９】


複製元
複製先
メモリカード110
携帯電話機100
携帯電話機102
メモリカード112
S316から
S322
コンテンツIDと{Dc}Kcを受理
S320
コンテンツIDと{Dc}Kcの出力要求をメモリカードへ入力
S324
{Dc}Kcを出力
S326
{Dc}Kcを受理し、複製先へ送信
S328
{Dc}Kcを受信し、メモリカードへ入力
S330
{Dc}Kcを受理し、メモリに記録
S304へ
S332
複製終了？
No
Yes
S334
ユーザにメッセージを表示
終了
S336

【図２０】



フロントページの続き

(51)Int.Cl.[7]	識別記号	F I		ﾃｰﾏｺｰﾄﾞ(参考)
G10K 15/02		G10K 15/02		
H04L 9/08		H04L 9/00	601B	